BY ORDER OF THE SUPERINTENDENT

HQ UNITED STATES AIR FORCE ACADEMY INSTRUCTION 17-101

7 JULY 2017

Cyberspace

INFORMATION TECHNOLOGY (IT) SERVICE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: HQ USAFA/A6

Certified by: HQ USAFA/A6 (Mr. David Hluska)

Supersedes: USAFAI33-101, 18 May 2011;
USAFAI33-115, 26 May 1011;
USAFAI33-116, 17 May 2011;
USAFAI33-117, 8 January 2013;
USAFAI33-118, 6 March 2013;
USAFAI33-119, 6 September 2011

Pages: 65

This instruction implements Department of Defense Directive (DODD) 8000.01, *Management of the DOD Information Enterprise*, DODD 8115.01, *Information Technology Portfolio Management*, DODD 8440.01, *Information Technology Service Management (ITSM), The DOD Enterprise Service Management Framework* (DESMF), and Air Force Instruction (AFI) 17-100, *Air Force Information Technology (IT) Service Management*. This instruction establishes the *Information Technology Infrastructure Library* (ITIL) as the key United States Air Force Academy (USAFA) IT governance framework. This publication provides direction for requesting, managing, maintaining, and controlling USAFA IT assets and systems. This publication does not apply to Air Force Reserve Command (AFRC) units nor the Air National Guard (ANG). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*. The authorities to waive requirements in this publication are identified with a Tier (T-3) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority. The waiver authority for non-tiered requirements in this publication is the USAFA Director of Communications and Information (HQ USAFA/A6). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW)

Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. Major changes include the consolidation of multiple USAFA 33 series instructions and the alignment of IT Service Management to the ITIL framework.

1. Scope and Purpose.

1.1. The purpose of this instruction is to provide an overarching document for USAFA IT Service Management (ITSM) and outline all IT practices, roles, responsibilities, policy, processes and function descriptions. It provides guidance to ensure delivery of IT services and management of the USAFA ITSM and aligns delivery of IT services with the mission, user satisfaction, and efficiency and needs of the organization. The processes outlined in this instruction apply international ITIL framework, standards, and best practices to ensure senior leaderships intent, direction, and policy expectations for IT are met, performance is measured, and that resources and risks are identified and managed. This policy ensures support to the USAFA IT Enterprise Schema as represented in Figure 1., 2., and 3., *USAFA IT Enterprise Schema.* This Schema is updated regularly and is available on the HQ USAFA/A6 SharePoint site.

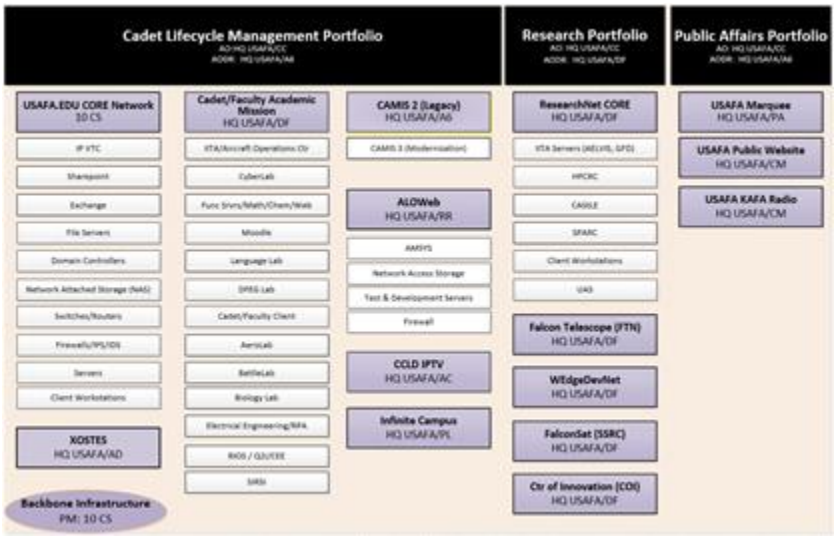
2. USAFA IT Enterprise Schema. The USAFA IT Enterprise Schema is a living document that could change based on technology, the IT Change Management Process and IT organization structure. The definitions below are based on systems at time of publication. Current Schema is located on the HQ USAFA/A6 SharePoint site at: Directorate of Communications and Information - Home.

2.1. Cadet Lifecycle Management Portfolio. This portfolio consists of systems unique to the academic mission of USAFA. The portfolio contains the USAFA.EDU core network, Academic Labs, Cadet Administrative Management Information System (CAMIS), and the Polaris Hall IPTV systems.

2.2. Research Portfolio. This portfolio consists of systems unique to academic research. Included in this portfolio is ResearchNet, IITA Servers, HPCRC, CAStLE, SPARC and UAS.

2.3. Public Affairs Portfolio. This portfolio consists of the USAFA Marquee, KAFA radio station, external website and official social media.

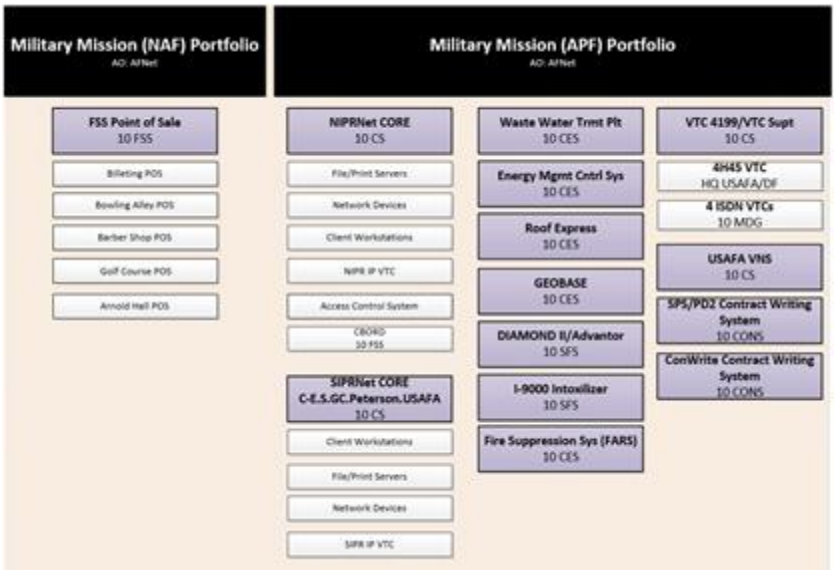
Figure 1. USAFA IT Enterprise Schema Section 1.



2.4. Military Mission Non-Appropriated Fund Portfolio. This portfolio consists of systems supporting the Morale, Welfare and Recreation mission of USAFA. It includes the 10th Force Support Squadron Point of Sale (POS), Billeting POS, Bowling Alley POS, Golf Course POS, Barber Shop POS and Arnold Hall POS.

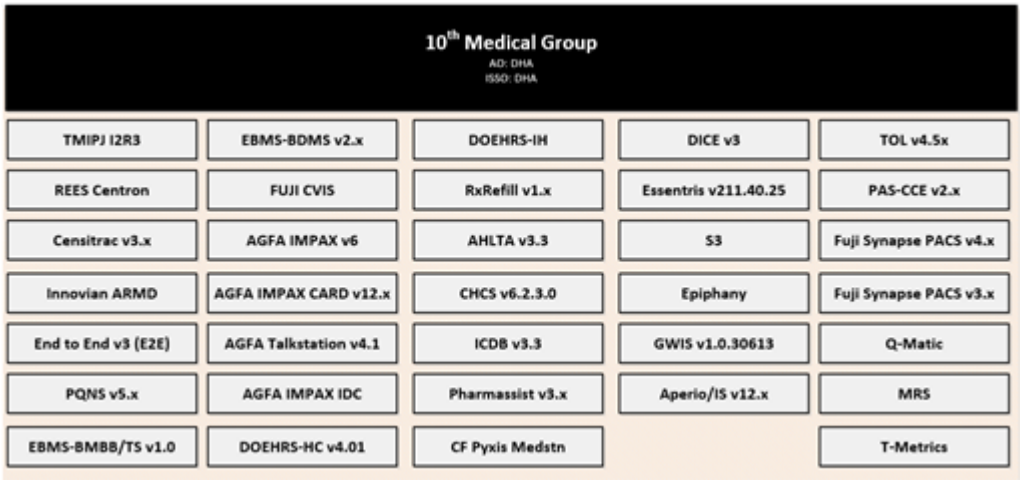
2.5. Military Mission Appropriated Fund Portfolio. This portfolio consists of systems that are part of the NIPRNet and SIPRNet core. These systems utilize AF funded infrastructure and are tied to the AFNet. Requests for changes to these systems will follow the processes outlined in this instruction; however additional approvals and actions may be needed from AF functional areas.

Figure 2. USAFA IT Enterprise Schema Section 2.



2.6. 10th Medical Group (10 MDG) Portfolio. This portfolio consists of systems unique to the medical support mission of the 10 MDG. Management of these systems is part of the Defense Health Agency. Requests for changes to these systems will follow the processes outlined in this instruction; however additional approvals and actions may be needed from AF functional areas.

Figure 3. USAFA IT Enterprise Schema Section 3.



2.7. Backbone Infrastructure Portfolio. This portfolio consists of infrastructure that is shared across multiple portfolios. It contains Inside Plant wiring, Outside Plant wiring, network devices, switches, routers and various shared appliances. Requests for changes to this portfolio will follow the processes outlined in this instruction; however additional approval and coordination may be required from AF functional areas and across Program Manager areas of responsibility.

3. Organizational Roles and Responsibilities. The roles and responsibilities listed in this instruction are unique to the USAFA IT Enterprise Schema. There may be other responsibilities required in Air Force instructions for general Information Technology Service Management that are not repeated in this publication.

3.1. The USAFA Superintendent (HQ USAFA/CC):

3.1.1. Is appointed by SAF-CIO/A6 as the Authorizing Official (AO) IAW AFI 17-130, *AF Cybersecurity Program Management*, for the Cadet Lifecycle Management Portfolio, Research Portfolio, and any new Portfolios under USAFA purview.

3.2. The USAFA Vice Superintendent (HQ USAFA/CV):

3.2.1. Will establish thresholds for Communications and Information (C&I) committee decisions and risk.

3.2.2. Will appoint Information System Owners (ISO) for all USAFA systems listed on the USAFA IT Enterprise Schema.

3.3. Mission Elements (ME) and Staff Directorates:

3.3.1. Nominate ISOs to HQ USAFA/CV for systems under their purview IAW the USAFA IT Enterprise Schema. If a ME or directorate does not have a system on the USAFA IT Enterprise Schema, there is no requirement to nominate an ISO.

3.3.2. Appoint Program Managers (PM) and Information System Security Officers (ISSO) for systems under their purview as listed on the USAFA IT Enterprise Schema. If a staff directorate or agency does not have a system on the USAFA IT Enterprise Schema, there is no requirement to nominate a PM or ISSO.

3.3.3. Appoint a C&I Committee member. The appointed C&I Committee member must be an ISO if the ME or directorate has a system. If the ME or directorate does not have any systems, they still must appoint a C&I committee member.

3.3.4. Appoint a Freedom of Information Act (FOIA) Monitor when requested by HQ USAFA/A6 (FOIA) office.

3.3.5. The USAFA Public Affairs office (HQ USAFA/PA) shall manage all aspects of the externally (public) facing content management programs IAW AFI 35-107, *Public Web Communications*.

3.3.6. Appoint a Communications Requirements Officer (CRO), unit Client Support Technician (CST), unit Cybersecurity Liaison (CL), Unit Software License Manager (USLM), SharePoint Site Collection Administrator (SPSCA), and Unit Privacy Monitor (UPA).

3.3.6.1. For the purpose of these requirements, the following should have CRO, CST, CL, USLM, SPSCA and UPAs:

3.3.6.1.1. HQ USAFA Staff

3.3.6.1.2. USAFA Dean of Faculty (HQ USAFA/DF) and each division (3-letter only)

3.3.6.1.3. USAFA Cadet Wing (HQ USAFA/CW) and each group (group level only)

3.3.6.1.4. Director of the Center for Character and Leadership Development (HQ USAFA/CWC)

3.3.6.1.5. USAFA Athletic Department (HQ USAFA/AD)

3.3.6.1.6. USAFA Preparatory School (HQ USAFA/PL)

3.3.6.1.7. A System PM may appoint a CRO or utilize the organization CRO

3.3.7. Ensure a Unit IT Property Manager is appointed to maintain roles in AFWay for IT purchasing IAW paragraph 6.7.

3.3.8. Provide POC information to 10th Communications Squadron (10 CS) for each distribution list under their purview.

3.3.9. Ensure Privacy Identifiable Information (PII) is not present in messages sent via mass distro lists IAW AFI 33-332. PII may be sent to Distro A only when encrypted. Any unencrypted address will not be sent PII.

3.4. The USAFA Director of Communications and Information (HQ USAFA/A6):

3.4.1. Is the focal point for all MAJCOM-level C&I functional issues and MAJCOM-level C&I requirements referenced in DOD and AF-level policy.

3.4.2. Develops, implements and publishes the USAFA IT Strategic Plan and the USAFA IT Enterprise Architecture.

3.4.3. Develops C&I policy and interprets higher-level C&I policy.

3.4.4. Ensures USAFA compliance with The Clinger-Cohen Act (CCA) -- Subtitle III of Title 40 United States Code, AFI 17-110, AF *Information Technology Portfolio Management and IT Investment*, and AFMAN 17-1402, *AF Clinger-Cohen Act (CCA) Compliance Guide*.

3.4.5. Appoints the USAFA Change Manager.

3.4.6. Appoints the USAFA Configuration Manager.

3.4.7. Nominates an ISO to HQ USAFA/CV for systems under HQ USAFA/A6 purview as listed on the USAFA IT Enterprise Schema.

3.4.8. Appoints the USAFA IT Financial Manager. The USAFA IT Financial Manager will oversee the IT Financial Management Process.

3.4.9. Appoints PMs and CLs for systems under HQ USAFA/A6 purview IAW the USAFA IT Enterprise Schema.

3.4.10. Organizes, trains and equips USAFA to execute the C&I mission.

3.4.10.1. Provides functional oversight for Enterprise-wide IT Manpower and Manning.

3.4.10.2. Prioritizes and recommends alignment of C&I manpower to meet USAFA mission requirements.

3.4.10.3. Ensures training and professional development is available to meet the needs of the C&I workforce.

3.4.11. Chairs the USAFA C&I Committee.

3.4.12. Provides Authorizing Official (AO) support for USAFA systems as listed on the USAFA IT Enterprise Schema.

3.4.13. Performs all MAJCOM-level and Wing-level Cybersecurity requirements IAW DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, AFI 17-130, and AFMAN 17-1303, *Cybersecurity Workforce Improvement Program.*

3.4.14. Performs MAJCOM and Wing-level roles for the Freedom of Information Act (FOIA), Privacy, Information Collection and Civil Liberties functions IAW DOD 5400.7-R_AFMAN 33-302, AFI 33-332, *AF Privacy and Civil Liberties Program*, and AFI 33-324, *The AF Information Collections and Reports Management Program*.

3.4.15. Develops USAFA Enterprise Information Management/Knowledge Management (EIM/KM) policy for content management, collection, control, creation, dissemination, and utilization of data, information, and knowledge across the USAFA enterprise.

3.4.15.1. Represents USAFA at Content Management AF level meetings and/or external (public) enterprise service events, completes content taskers on behalf of USAFA, provides representative for AF Integrated Product Teams, and works with external agencies.

3.4.15.2. Seeks out opportunities for improvement and enhancement of system capabilities and Content Management programs on behalf of USAFA.

3.4.16. Operates and Maintains systems listed under HQ USAFA/A6 purview IAW the USAFA IT Enterprise Schema.

3.4.17. Ensures applications and systems are available to provide the required functionality for IT services. This includes the development and maintenance of custom applications, as well as, the customization of products from software vendors.

3.5. Unit Commanders and Directors:

3.5.1. Appoint a CRO, unit CST, unit CL, USLM, SPSCA, UPA and FOIA monitor.

3.5.1.1. For the purpose of these requirements, the following should have CRO, CST, CL, USLM, SPSCA and UPAs.

3.5.1.1.1. 10th Air Base Wing (10 ABW) Staff

3.5.1.1.2. 10th Mission Support Group (10 MSG)

3.5.1.1.3. 10 MDG

3.5.1.1.4. Each squadron (optional)

3.5.1.1.5. Each Tenant unit

3.5.2. Ensure a Unit IT Property Manager is appointed to maintain roles in AFWay for IT purchasing IAW paragraph 6.7.

3.5.3. Provide POC information to 10 CS for each distribution list under their purview.

3.5.4. Ensure PII is not present in messages sent via mass distro lists IAW AFI 33-332. PII may be sent to Distro A only when encrypted. Any unencrypted address will not be sent PII.

3.6. Director, 10 CS (10 CS/CL):

3.6.1. Operates and maintains all C&I systems, infrastructure and applications under 10 CS purview IAW the USAFA IT Enterprise Schema.

3.6.1.1. Maintains shared IT infrastructure for all USAFA Core Systems as listed on the USAFA IT Enterprise Schema.

3.6.2. Creates and maintains a Communications Focal Point (CFP) to provide the function of the Service Desk as defined in paragraph 8.2.

3.6.3. Appoints the USAFA Change Coordinator.

3.6.4. Identify a participant for the Air Force Knowledge Management Working Group (AFKMWG) IAW AFI 33-396, *Knowledge Management*.

3.6.5. Ensures downward directed and internally generated Request for Change (RFC) are entered into the Cyberspace Infrastructure Planning System (CIPS).

3.6.6. Creates, maintains and provides access to the USAFA IT Service Catalog IAW Attachment 2.

3.6.7. Oversees Project Management for changes to systems, infrastructure or applications under 10 CS purview IAW USAFA IT Enterprise Schema. Ensures all applicable IT projects have a Project Manager (PjM) assigned.

3.6.8. Develops, maintains and coordinates IT Service Level Agreements (SLA) between 10 CS and other system PMs.

3.6.9. Maintains a test environment.

3.6.10. Ensures all RFCs have been vetted IAW the IT Change Management Process, paragraph 7.3. before being loaded to the live environment.

3.6.11. Ensures the appropriate Functional System Administrator (FSA) takes actions such as disconnect/isolate systems to mitigate the risks of any network vulnerability occurrence.

3.6.12. Acknowledge, disseminate, implement, track and report compliance with Security Technical Implementation Guides (STIG), TCNOs and C4 NOTAMs on the .MIL network.

3.6.13. Ensures personnel develop and maintain the skills and certifications required to operate IT infrastructure and systems IAW DOD 8570.01-M and AFMAN 17-1303.

3.6.14. Develops and maintains client images for all systems under their purview.

4. Functional Roles and Responsibilities.

4.1. USAFA Authorizing Official (AO) will:

4.1.1. Perform the duties of the AO IAW AFI 17-101, *Risk Management Framework (RMF) for AF Information Technology,* and AFI 17-130.

4.1.2. Approve assessment and accept residual risk for systems under USAFA AO purview IAW the USAFA IT Enterprise Schema.

4.1.3. Grant Authority to Operate (ATO) or Denial of Authority to Operate (DATO) for systems under AO purview. The USAFA AO may only accept residual risk for systems with open category (CAT) II and III findings. SAF CIO is the only authority authorized to accept residual risk for systems with CAT I findings.

4.1.4. Complete Defense Information Systems Agency (DISA) AO training IAW DOD 8570.01-M and AFMAN 17-1303. Proof of training certificate will be included as an artifact to system assessment packages.

4.1.5. Appoint AO Designated Representatives (AODR) to support the assessment process for systems under AO purview as listed on the USAFA IT Enterprise Schema.

4.1.6. These responsibilities may not be further delegated.

4.2. Authorizing Official Designated Representative (AODR):

4.2.1. Complete DISA AO training IAW DOD 8570.01-M and AFMAN 17-1303. Proof of training certificate will be included as an artifact to system assessment packages.

4.2.2. Make assessment recommendations to the USAFA AO based on input and validation of cybersecurity controls from the Security Control Assessor (SCA).

4.2.3. Perform all responsibilities as outlined by the AO except formally accept risk for a system. An AODR is not authorized to approve assessment for any system.

4.2.4. HQ USAFA/A6, shall perform duties as AODR for all USAFA-owned networks, excluding ResearchNet and ResearchNet Sub-enclaves.

4.2.5. The Director of the High Performance Computing Research Center (HQ USAFA/DFAN) shall perform duties as AODR for the ResearchNet and ResearchNet sub-enclaves.

4.3. Security Control Assessor (SCA):

4.3.1. Is appointed by SAF-CIO/A6 as the SCA IAW AFI 17-130.

4.3.2. Completes training and maintains appropriate cybersecurity certification IAW DOD 8570.01-M and AFMAN 17-1303.

4.3.3. Determines Risk Categorization for all USAFA systems IAW DODI 8510.01, *Risk Management Framework for DOD Information Technology*.

4.3.4. Analyzes system assessment packages for risk, and develops risk-based recommendations for USAFA AO approval.

4.3.5. Provides final risk recommendations to support AO assessment decisions.

4.4. USAFA IT Information System Owners (ISO):

4.4.1. Ensure resource requirements for Information Systems under their purview IAW the USAFA IT Enterprise Schema are identified and systems comply with cybersecurity laws and policy.

4.4.2. Verify system data for Information Systems under their purview is recorded in AF Information Technology Investment Portfolio (ITIP).

4.4.3. Ensure Information Systems under their purview are operating in accordance with security requirements.

4.4.4. Review Assessment and Authorization (A&A) packages in Enterprise Mission Assurance Support Service (eMASS) for Information Systems under their purview.

4.4.5. Perform ISO cybersecurity duties IAW AFI 17-130.

4.5. Core Program Managers. Core Systems are noted as such on the USAFA IT Enterprise Schema.

4.5.1. Oversee the Warranty, Reliability, Maintainability, and Redundancy of Core Networks under their purview IAW the USAFA IT Enterprise Schema.

4.5.2. Manage, document and execute Demand Management, Service Level Management, Transition Planning and Support, Incident Management, Problem Management, and Access Management processes for systems under their purview IAW the USAFA IT Enterprise Schema.

4.5.3. Manage and maintain a Configuration Management System (CMS) for systems under their purview.

4.5.4. Manage and maintain a system baseline architecture or a description of the essential components of a service/system and document in the CMS for systems under their purview.

4.5.5. Develop, manage and coordinate Service Level Agreements with 10 CS or other affected system PMs for management of servers, applications, services or systems that connect to systems under their purview.

4.5.6. Provide information to be included in the USAFA IT Service Catalog for systems under their purview.

4.5.7. Manage and maintain a system Availability Management Process.

4.5.7.1. Define, analyze, plan, measure, and improve all aspects of the availability of IT services under their purview.

4.5.7.2. Ensure that all IT infrastructure, processes, tools, etc. are appropriate for the agreed service availability target level.

4.5.7.3. Work closely with MEs and Staff Directorates to identify 'event driven' circumstances that impact system availability.

4.5.7.4. Work closely with 10 CS to review latency issues and concerns to ensure sufficient bandwidth to meet the required demand.

4.5.8. Manage and maintain a Capacity Management Process for systems under their purview.

4.5.8.1. Ensure services and infrastructure are able to deliver the agreed capacity and performance targets in a cost effective and timely manner.

4.5.8.2. Consider resources required to deliver services, and plans for short, medium and long term requirements.

4.5.8.3. Accomplish long term trend analysis of system and identifies future constraints.

4.5.9. Manage and maintain a continuity management process for systems under their purview.

4.5.9.1. Prepare a continuity of operations plan (COOP) identifying the resources necessary to support required IT services in the event of natural disasters, mechanical failures, terrorist acts, etc.

4.5.9.2. Perform risk minimizing precautions for disaster situations to reduce risk to acceptable levels.

4.5.9.3. Ensure that minimum agreed service levels are provided in cases of disaster

4.5.9.4. Plan for continued service in case of evacuation or impeded access to managed servers.

4.5.9.5. Manage and maintain a Vulnerability Management Plan (VMP) for each applicable system and file it as part of the USAFA IT Enterprise VMP.

4.5.9.5.1. The plan will contain identification and mitigation process for network vulnerabilities posing threats to systems and information.

4.5.9.5.2. Align the VMP with specific procedures published in MPTO 00-33A-1109, *Air Force Information Network (AFIN) Vulnerability Management,* as applicable for each system.

4.5.9.6. Acknowledge, disseminate, implement, track, assess and report compliance with STIGs, Information Assurance Vulnerability Managements (IAVM), TCNOs and C4 NOTAMs on the .MIL network IAW the USAFA IT Enterprise VMP.

4.5.10. Manage and maintain an Event Management Process for systems under their purview.

4.5.10.1. Manage and maintain event monitoring tools.

4.5.10.2. Identify exact targets and mechanisms for monitoring.

4.5.10.3. Define what can and needs to be monitored.

4.5.10.4. Define what type of monitoring is required.

4.5.10.5. Define what data shall be used to populate the appropriate event record.

4.6. All Program Managers:

4.6.1. Manage the application and operation functions for systems under their purview IAW the USAFA IT Enterprise Schema.

4.6.2. Manage, document, and operate the processes covering Access Management, Event Management, Incident Management, Problem Management, and Service Request Management for systems under their purview.

4.6.3. Coordinate Service Level Agreements with 10 CS or Core Network PMs for systems under their purview.

4.6.4. Appoint a FSA for each system under their purview.

4.6.5. Ensure systems under their purview are accredited IAW AFI 17-101, AFI 17-130, and paragraph 7.5.

4.6.5.1. Ensure A&A documentation is kept current IAW AFI 17-101 and AFI 17-130.

4.6.6. Ensure funding for each system under their purview is properly programmed in the Program Objectives Memorandum (POM), budgeted and executed IAW the USAFA Planning, Programming, Budget, Execution (PPB&E).

4.6.6.1. Ensure all lifecycle costs are accounted for and addressed in the PPB&E.

4.6.7. Manage a Lifecycle Replacement (LCR) plan for system IT equipment under their purview. Work with 10 CS for LCR of client systems.

4.6.8. Attend the Change Advisor Working Group (CAWG), IT Financial Working Group (ITFWG), and Cybersecurity Working Group (CSWG) as a primary member.

4.6.9. Implement a risk vulnerability management process that ensures identification and mitigation of network vulnerabilities posing threats to systems and information. Provide process information to Core PM to include in the system VMP.

4.6.10. Acknowledge, disseminate, implement, track and report compliance with STIGs, TCNOs and C4 NOTAMs systems under their purview.

4.6.11. Review all IAVMs received for implementation and evaluate for feasibility.

4.6.11.1. Implement IAVMs on systems under their purview.

4.6.11.2. Report to Cybersecurity any IAVM exceptions, variances, or mitigations and document in the Plan of Action and Milestone (POA&M) any deviations.

4.6.12. Ensure an IT Change Management Process exists for systems under their purview. Any change that impacts CORE USAFA systems or any IT purchase must utilize the USAFA IT Change Management Process outlined in this instruction.

4.6.13. Manage systems under their purview throughout the system lifecycle; design, test, and operation.

4.7. The USAFA Change Manager:

4.7.1. Oversee the IT Change Management Process for core systems IAW the USAFA IT Enterprise Schema.

4.7.2. Convene and chair the CAWG.

4.7.3. Publish CAWG Agenda no later than 1 business day prior to CAWG meeting. Agenda shall include all RFCs under review.

4.7.4. Publish and maintain CAWG minutes IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

4.8. The USAFA Configuration Manager shall:

4.8.1. Provide oversight for the Configuration Management process and aid in the resolution of conflicts requiring a higher authority.

4.8.2. Attend the C&I Committee as a primary member.

4.8.3. Convene and chair the USAFA Configuration Control Working Group (CCWG).

4.8.4. Exercise oversight over what level of Configuration Management is required for services, projects, assets and documentation, and how this level shall be achieved.

4.8.5. Exercise oversight over configuration control requirements for each accredited system in coordination with the assigned PM.

4.8.6. Ensure configuration changes affecting USAFA systems are reviewed and approved at the CCWG when appropriate.

4.8.7. Complete analysis of RFCs, Service Design Packages (SDP) and other inputs for review by the CCWG, CAWG and Change Manager.

4.8.8. Notify the Change Manager of relevant CCWG decisions.

4.9. USAFA Chief Technology Officer /Enterprise Architect (CTO) shall review all systems for validation against enterprise architecture, integration and operational planning requirements. The CTO may require additional documentation and justification to meet DOD architectural framework requirements and compliance.

4.10. USAFA Portfolio Manager shall:

4.10.1. Maintain a USAFA Service Portfolio that is a complete listing of IT services and investments managed by USAFA.

4.10.2. Ensure USAFA C&I investments are maintained in the ITIP IAW AFI 17-110.

4.10.3. Provide guidance, tracking and oversight to report program status in ITIP and determine if other program reviews/approval are required.

4.10.4. Ensure that the USAFA portfolio reflects the appropriate level of investment for service mix.

4.10.5. Coordinate with PMs to gather all necessary documentation IAW federal compliance processes (e.g. ITIP, Federal Information Security Management Act, Clinger Cohen Act, Sarbanes-Oakley, National Defense Acquisition Act).

4.10.6. Reviews ITIP inputs for RFCs as part of the IT Change Management Process.

4.11. The USAFA Information System Security Manager (ISSM) shall:

4.11.1. Develop, implement, oversee, and maintain a comprehensive cybersecurity program identifying cybersecurity architecture, security requirements, objectives, policies, and personnel IAW AFI 17-101, AFI 17-130, AFMAN 17-1301, *Computer Security (COMPUSEC),* and AFMAN 17-1303.

4.11.2. Oversee the IAVM program IAW MPTO 00-33A-1109..

4.11.3. Provide oversight and management of the USAFA Cybersecurity Office.

4.11.4. Monitor Cybersecurity Certification Requirements.

4.11.5. Maintain active membership on the Air Force Cybersecurity Technical Advisory Group (AFCTAG).

4.11.6. Brief, with coordination of the SCA, the AO on all initial and recurring A&A packages requiring AO approval.

4.11.7. Review USAFA contract performance work statements for cybersecurity concerns and compliance.

4.11.8. Prepare an annual budget submission for training and certification of all military and civilian personnel identified as part of the cybersecurity workforce.

4.11.9. Performs duties IAW AFI 17-130 as the Security Control Assessor Representative (SCAR).

4.12. USAFA Cybersecurity Office shall:

4.12.1. Manage the cybersecurity programs base-wide, by providing guidance and oversight for new and existing systems, configuration changes to the security baseline, POA&M mitigations for assessment packages and A&A packages.

4.12.2. Coordinate with ISOs and PMs of new systems to identify security requirements.

4.12.3. Ensure risk assessments are conducted for all new and existing systems. Conduct scans using DISA approved tools to identify vulnerabilities.

4.12.4. Develop and maintain a USAFA IT Enterprise Cyber Incident Response Plan (CIRP).

4.12.5. Maintain ISSO and FSA appointment letters and revalidate annually.

4.12.6. Manage the USAFA Approved Software List (ASL).

4.12.7. Conduct security testing and analysis of new applications/software.

4.12.8. Provide cybersecurity input to all Work Order/RFC tickets as applicable.

4.12.9. Complete A&A actions IAW AFI 17-101.

4.12.10. Review and approve system VMPs.

4.12.11. Record and track all approved IAVM exceptions, variances, or mitigations.

4.12.12. Maintain signed USAFA Form 75, *Privileged User Agreements,* for personnel with privileged access.

4.12.13. Ensure applications/software of any kind are not developed, implemented, nor operated outside of an accredited system.

4.12.14. Ensure applications/software are scanned and tested for cybersecurity requirements before deployment.

4.13. Enterprise Information Systems PM shall:

4.13.1. Oversee the USAFA level EIS requirements, programs, resources, and acquisitions.

4.13.2. Manage USAFA content management in coordination with HQ USAFA/PA.

4.13.3. Coordinate on USAFA's Strategic vision, plans, and resources for content management issues.

4.13.4. Submit requests to centrally manage unsupported Content Management resources, unfunded requirements, Program Objectives Memorandum (POM) and new USAFA focused Content Management program requirements.

4.13.5. Review all Content Management programs (and new requests) for required tracking, efficiencies, and compliance.

4.14. USAFA Chief of Privacy shall:

4.14.1. Review all Content Management programs initially for possible Privacy Impact Assessment (PIA), System of Record Notice (SORN), legal tracking or compliance requirements.

4.14.2. Manage the USAFA FOIA, Privacy, Information Collection and Civil Liberties programs IAW DOD 5400.7-R_AFMAN 33-302, AFI 33-332, and AFI 33-324.

4.15. USAFA Change Coordinator:

4.15.1. Ensure all change requests have a completed and valid Work Order/RFC submission prior to processing.

4.15.2. Control the lifecycle of change. Ensure all change requests are assessed, recorded, categorized, planned, evaluated, approved, scheduled, tested, implemented, reviewed and closed in a controlled manner.

4.15.3. Determine the appropriate change process for valid Work Order/RFC submissions IAW the IT Change Management Process.

4.15.4. Oversee the Standard, Minor and Emergency Change processes.

4.15.5. Ensure changes are documented and tracked throughout their lifecycle.

4.15.6. Maintain a Change priority list to present and vet before the CAWG.

4.15.7. Create, maintain, and publish the change schedule to include Authorized Service Interruptions (ASI).

4.15.8. Attend the CAWG as a primary member.

4.15.9. Provide the Change Manager with a Monthly Change Report that lists all approved and disapproved Emergency and Minor Changes.

4.15.10. Ensure procedures for MPTO 00-33A-1100, *AFNet Operations Change Management Process,* and AFMAN 33-402, *Service Development and Delivery Process (SDDP),* are followed when appropriate.

4.16. Functional System Administrators (FSA):

4.16.1. Responsible for patches and IAVM of systems unless otherwise stated in an SLA or contract PWS.

4.16.2. Maintain systems under their purview as assigned by PM.

4.16.3. Configure and operate system according to cybersecurity policies and procedures and notifies the AO, ISSM or ISSO of any changes that might adversely impact cybersecurity.

4.16.4. Ensure IT under their management is properly patched.

4.16.5. Establish and manages authorized user accounts for system under their purview; including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

4.16.6. Mitigate all CAT I vulnerabilities IAW STIG and IAVM requirements on assigned systems.

4.16.7. Mitigate all CAT II and CAT III vulnerabilities IAW DODI 8500.01, *Cybersecurity*, DOD 8510.01, DISA STIGs, and IAVM requirements on assigned systems.

4.16.8. Request exceptions or variances to CAT III findings/vulnerabilities IAW the IT Change Management Process.

4.16.9. Conduct and document annual cybersecurity inspection of their system. Provide report to Cybersecurity annually.

4.17. Unit Cybersecurity Liaisons (CL):

4.17.1. All units must comply with MPTO 00-33A-1112, *Air Force Network Enterprise Service Desk Service Incident Management*, AFI 17-203, *Cyber Incident Handling,* and AFMAN 17-1301. The CL duties may be absorbed into the duties of the unit orderly room with a point of contact provided to the Cybersecurity Office. Whether the position is appointed or a part of the overall orderly room the following duties must be performed:

4.17.2. Request and maintain access to AF system (currently IAO Express) for user account management.

4.17.3. Use AF system to request user accounts for unit personnel.

4.17.3.1. Ensure all users have the requisite security clearances, supervisory need-to-know authorization, and awareness of their cybersecurity responsibilities (via cybersecurity training) before being granted access to Air Force IT.

4.17.3.2. Maintain all IS authorized user access control documentation IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

4.17.4. Report cybersecurity incidents or vulnerabilities to the cybersecurity office.

4.17.5. In coordination with the cybersecurity office, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered.

4.18. Communications Requirements Officer (CRO):

4.18.1. Submit validated IT requirements in CIPS on behalf of their ME, Directorate, Staff Agency, Unit or PM.

4.18.2. Ensure all required information is included in the CIPS work order as stated in paragraph 7.3.1.1.2.

4.18.3. Provide status of Work Order/RFC to requesters.

4.19. Computer Support Technician (CST):

4.19.1. Join computers to their systems/domains, add printers, add/remove enterprise or approved software, perform minor computer and peripheral troubleshooting, wipe hard drives (using AF-approved software) prior to equipment turn-in and assist users with their accounts.

4.20. SharePoint Site Collection Administrators (SPSCA) shall:

4.20.1. Manage content IAW AFI 17-100, AFMAN 17-1202, *Collaboration Services and Voice Systems Management*, and the Discovery and Information Management Technical Order (when published).

4.20.2. Complete Enterprise Information Systems PM recommended SharePoint training.

4.20.3. Manage internal (private) facing content.

4.20.4. Manage SharePoint sites for respective ME, directorate, unit, staff agency, tenant or organization.

4.20.4.1. Conduct day-to-day administration and support of their assigned sites.

4.20.4.2. Ensure each site collection includes the name and phone number of primary and alternate SPSCA

4.20.4.3. Conduct content review for stagnant data and cleanup of the respective assigned site.

4.20.4.4. Manage the creation, appointment and administration of sub-sites and Content Owners.

4.20.4.5. Delete unused SharePoint sites and workspaces if they have been inactive for 180 days or more as necessary.

4.20.4.6. Ensure sites have the required permissions and access to appropriately manage and protect information.

4.20.4.7. Ensure the assigned site is compliant with AFI 17-130, AFI 17-201, *Command and Control (C2) for Cyberspace Operations*, and AFI 33-332.

4.21. Content Owners and Contributors:

4.21.1. Manage the individual sub-sites within a site collection of internal (private) facing content that represents a specific ME/unit/org or project.

4.21.2. Provide end users training on their specific site and structure (as needed).

4.21.3. Conduct a content review for stagnant data and cleanup of their respective sites.

4.21.4. Ensure sites have the required permissions and access set up to appropriately manage and protect information.

4.21.5. Ensure the assigned site is compliant with AFI 17-130, AFI 17-201, and AFI 33-332.

4.22. All USAFA IT Users and Customers shall:

4.22.1. Submit IT Service Change Requests and Requirements to their respective CRO. Trouble tickets may be submitted via the CFP.

4.22.2. Submit all IT incidents to the CFP via Remedy/vESD/email/phone as appropriate.

4.22.3. Comply with guidance in AFMAN 17-1201, *User Responsibilities and Guidance for Information Systems*.

4.22.4. Accept government monitoring and security vulnerability scans, when accessing government sites such as USAFA .EDU, while using privately-owned Cadet computers.

4.22.5. Minimize the use of images or attachments by using hyperlinks in order to save bandwidth and email box storage capability.

4.22.6. Ensure that they are running anti-virus software with current antivirus signatures from 10 CS and/or PM, and scan all removable media prior to use.

4.22.7. Refrain from using exact deployment/leave/TDY dates, deployment/leave/TDY locations, description/nature of absence, or any personal details that might lead to exploitation when creating an out-of-office email/voicemail.

4.22.8. Not use the network to interfere with system security or integrity, obstruct users from authorized services, nor conduct harassing activities toward other network users.

4.22.9. Not release malware or a program that negatively impacts a system and/or hinders other computing devices.

4.22.10. Not tap phone or network lines.

4.22.11. Not establish any non-approved remote access and connections to servers or personal computers on the USAFA .EDU network without authorization.

4.22.12. Not send junk mail, chain letters, ghost writing email, use email resources to disrupt or overload mail services within or outside USAFA via "email bombing" or "spamming."

4.22.13. Not broadcast unsubstantiated virus warnings.

4.22.14. Not take any action while intentionally trying to be anonymous or untraceable (e.g., **www.unblockict.com**, uprox.com, TOR, anonymizer.com, etc.).

4.22.15. Not install, configure or use any peer-to-peer, personal proxy, or (Voice Over IP such as MagicJack, Skype (except as included in the default Microsoft Windows OS baseline), Vonage, etc.) software including, but not limited to Kazaa, Gnutella, Morpheus, MP3 Voyeur, Grokster, eDonkey, CC Proxy, FreeProxy, NetConceal Anonymizer, Anonymity 4, etc.

4.22.16. Not connect computer to the USAFA network while simultaneously using modems or wireless cards to access another networks (i.e. Verizon, AT&T, Sprint Broadband cards).

4.22.17. Ensure only government-procured removable media and storage devices are used in government-furnished computer systems connected to USAFA government networks.

4.22.17.1. Not use any USB/Flash media drives/removable storage device that does not meet DoD and AF guidance on any computer connected to a USAFA network or risk item confiscation.

4.22.18. Ensure PII is not present in messages sent via mass distro lists IAW AFI 33-332. PII may be sent to Distro A only when encrypted. Any unencrypted address will not be sent PII.

5. Service Strategy. Service Strategy determines which types of services should be offered to which customers. Service Portfolio Management, IT Financial Management, Business Relationship Management, IT Strategy Management and Demand Management make up USAFA's Service Strategy Policy.

5.1. Service Portfolio Management. Service Portfolio Management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. HQ USAFA/A6 owns the Service Portfolio Management process.

5.2. IT Financial Management. IT Financial Management manages the budgeting and accounting of IT requirements. It involves the development of policy and procedures to maximize efficiencies and reduce risks of C&I acquisitions. This process also integrates USAFA PPB&E, financial management processes and the 10th Contracting Squadron (10 CONS) purchasing and contracting processes. HQ USAFA/A6 owns the IT Financial Management process. This process is controlled by the IT Financial Working Group (ITFWG).

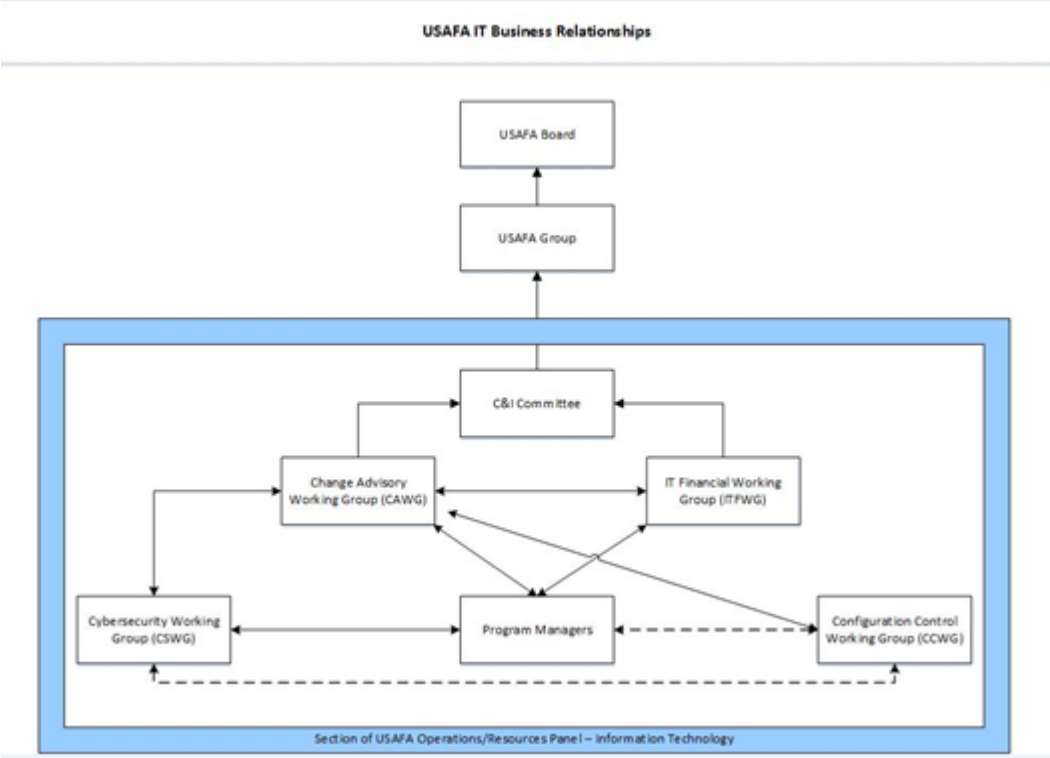
5.2.1. The IT Financial Manager shall consolidate all IT Enterprise requirements and advocate for funding (via the ITFWG and USAFA Financial Management's (HQ USAFA/FM) financial processes).

5.2.2. The IT Financial Manager will coordinate with USAFA/FM to ensure funds are disbursed IAW IT requirements and proper elements of expense.

5.3. Business Relationship Management (BRM). Business Relationship Management identifies the needs of existing and potential customers and ensures that appropriate services are developed to meet those needs and maintain a positive relationship. Figure 4. is a visual representation of the C&I BRM relationships.

5.3.1. C&I decisions at USAFA follow the USAFA Corporate Process Structure. In that structure, USAFA has a decision making hierarchy consisting of the USAFA Board, the USAFA Group Panel, multiple Panels, Committees and Working Groups. The USAFA C&I Committee is part of the USAFA Operations Panel and has multiple subordinate Working Groups. C&I decisions are made at the lowest level of the USAFA Corporate Structure according to established thresholds.

Figure 4. USAFA IT Business Relationships.



5.3.2. Communications and Information (C&I) Committee

5.3.2.1. The C& I Committee serves as the sole entry point to the USAFA Operations/Resource Panel, USAFA Group and USAFA Board for all C&I decisions. All C&I issues requiring USAFA Group or Board decisions will first be vetted through the C&I Committee.

5.3.2.2. HQ USAFA/A6 will chair the C&I Committee.

Table 1. C&I Committee membership.

Primary Members	Secondary Members
USAFA CTO /Enterprise Architect	HQ USAFA/A6 Staff
USAFA Portfolio Manager	Secondary ISOs from the MEs
One appointed ISO from each ME	PMs
One appointed ISO from each HQ Staff Directorate with an accredited system	HQ USAFA/FM
10 CS/CL	Director, 10 CONS
	Invited guests of the HQ USAFA/A6

5.3.2.3. A quorum is achieved if five primary members are present.

5.3.2.4. The C&I Committee will convene quarterly (or as needed) to review recommendations and decisions from subordinate working groups, coordinate on C&I policy changes, establish the ME/Directorate C&I funding baseline, approve C&I requirements above the ME/Directorate baseline for additional funding consideration, approve requirements submitted by HQ USAFA/FM, monitor C&I Spending/Execution Plans throughout the fiscal year (as required as a result of Program Management Review), review annual C&I financial plans, approve major C&I portfolio changes or investment decisions, prioritize C&I unfunded requirements, coordinate on the HQ USAFA/A6 Enterprise IT Strategy and Roadmap and prioritize IT resources and requirements.

5.3.2.5. The C&I Committee will establish Enterprise C&I Strategic Goals and supporting Program Objective Memorandum (POM) inputs.

5.3.2.6. Decisions above the established C&I Committee decision threshold and any unresolved issues will be elevated to the USAFA Operations Panel and USAFA Group Panel for resolution.

5.3.2.7. HQ USAFA/A6 shall ensure C&I Committee meeting minutes are recorded and maintained IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

5.3.3. Change Advisory Working Group (CAWG).

5.3.3.1. The CAWG reviews significant change requirements and other issues as determined by the USAFA Change Manager.

5.3.3.2. The USAFA Change Manager will chair the CAWG.

Table 2. CAWG membership.

Primary Members	Secondary Members
USAFA Change Coordinator	HQ USAFA/A6 Staff
10 CS/SCO (representing operations management, service catalog and demand management)	Unit CROs
USAFA Configuration Manager	USAFA Chief of Privacy
USAFA Portfolio Manager	Invited guests of the USAFA Change Manager
USAFA ISSM	Project Managers
System PMs	

5.3.3.3. The CAWG meets monthly and as required.

5.3.3.4. The CAWG approves, disapproves or elevates issues to the C&I Committee as appropriate.

5.3.3.5. The CAWG reviews Change Requests for impact on the USAFA Mission, IT infrastructure, existing services, resources, IT Architecture, IT Configuration, IT Strategic Plan, and IT Strategic Roadmap IAW the IT Change Management Process.

5.3.3.6. The CAWG will prioritize RFCs to maximize success and support of overall USAFA IT projects.

5.3.3.7. Decisions above the established CAWG decision threshold and any unresolved issues will be elevated to the C&I Committee for resolution.

5.3.3.8. The USAFA Change Manager shall ensure CAWG meeting minutes are recorded and maintained IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

5.3.4. IT Financial Working Group (ITFWG).

5.3.4.1. The ITFWG reviews C&I requirements submitted to HQ USAFA/FM each Fiscal Year and determines final submission.

5.3.4.2. The USAFA IT Financial Manager will chair the ITFWG.

Table 3. ITFWG membership.

Primary Members	Secondary Members
System PMs	HQ USAFA/A6 Staff
HQ Staff Directorates and MEs without a PM may appoint a non-PM as a primary member	ME Resource Advisors
	HQ USAFA/FM representative
	10 CONS representative
	Invited guests of the IT Financial Manager

5.3.4.3. The ITFWG meets quarterly or as required to meet USAFA needs.

5.3.4.4. The ITFWG determines ME/Directorate C&I Funding Baseline.

5.3.4.5. The ITFWG provides consolidated USAFA C&I input to the USAFA PPB&E process.

5.3.4.6. The ITFWG reviews and prioritizes C&I unfunded requirements for to submit to USAFA/FM for addition fund sourcing.

5.3.4.7. The ITFWG reviews and monitors C&I Spending/Execution Plans throughout the Fiscal Year.

5.3.4.8. The ITFWG determine out-year C&I requirements as part of the Corporate Program Objective Memorandum (POM) process.

5.3.4.9. The ITFWG prepares and submits IT portfolio investments in the annual budget estimate and presidential budget submissions and advocates for funding via the ITFWG and HQ USAFA/FM's financial processes.

5.3.4.10. Decisions above the established ITFWG decision threshold and any unresolved issues will be elevated to the C&I Committee for resolution.

5.3.4.11. The IT Financial Manager shall ensure ITFWG meeting minutes are recorded and maintained IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

5.3.5. Cybersecurity Working Group (CSWG).

5.3.5.1. The CSWG formulates recommendations based on mission impact and Cybersecurity to the USAFA Change Manager when requested IAW USAFA IT Change Management Process.

5.3.5.2. The USAFA ISSM will chair the CSWG.

Table 4. CSWG membership.

Primary Members	Secondary Members
System PMs	HQ USAFA/A6 Staff
ISSOs	USAFA Information Protection (HQ USAFA/IP)
10 CS Boundary Protection	USAFA Operations Security (OPSEC)
10 CS Network Defense	Invited guests of the USAFA ISSM
10 CS Information Protection Operations	

5.3.5.3. The CSWG meets monthly and as required.

5.3.5.4. The CSWG will review all downward directed security measures to determine impact on USAFA systems. The CSWG will recommend approval/disapproval to the USAFA Change Manager.

5.3.5.5. The USAFA ISSM shall ensure CSWG meeting minutes are recorded and maintained IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

5.3.6. Configuration Control Working Group (CCWG).

5.3.6.1. The CCWG will provide technical review and advice to the USAFA Change Manager on changes to Configuration Items (CIs) in the USAFA IT Enterprise as determined by the USAFA Configuration Manager. This information includes relationships between CIs, system documentation, diagrams, and Service Level Agreements (SLAs).

5.3.6.2. The USAFA Configuration Manager will chair the CCWG.

Table 5. CCWG membership.

Primary Members	Secondary Members
10 CS/SCX Flight Chief	HQ USAFA/A6 Staff
10 CS/SCO Flight Chief	System PM/PjM submitting RFC
10 CS IT Engineer	ME CROs
USAFA Portfolio Manager	Invited guests of the USAFA Configuration Manager
USAFA ISSM	

5.3.6.3. The CCWG meets as required.

5.3.6.4. The CCWG formulates recommendations on technical feasibility, impact, and risk associated with a significant change IAW the USAFA IT Change Management Process.

5.3.6.5. Recommendations are recorded in the RFC record and CCWG meeting minutes and forwarded to the Change Manager for review.

5.3.6.6. The USAFA Configuration Manager shall ensure CCWG minutes are recorded and maintained IAW AFMAN 33-363 and disposed of IAW AFRIMS RDS.

5.4. IT Strategy Management. Strategy Management involves the assessment of IT offerings and capabilities in order to develop a strategy to serve customers. Once the strategy has been defined, IT Strategy Management also includes implementation and maintenance of the strategy. HQ USAFA/A6 owns the IT Strategy for USAFA.

5.5. Demand Management. Demand Management works with Capacity Management to ensure that there is sufficient capacity to meet the required demand.

5.5.1. PMs shall develop, document, and execute a process to monitor and forecast demand for IT Services based upon Service Strategy, requests from IT service consumers, and historic consumption trends. The Demand Management process includes:

5.5.1.1. Monitoring and managing the cyclical use, capacity, and latency of IT services, influencing customer demand for services where appropriate.

5.5.1.2. Working closely with capacity management to ensure that sufficient capacity exists to meet the required demand.

5.5.1.3. Reviewing latency issues to ensure sufficient bandwidth to meet the required demand.

5.5.1.4. Working closely with MEs and Staff Directorates to identify 'event driven' circumstances that impact demand for products and services.

5.5.1.5. Recommending updates or upgrades based on usage history and forecasts.

5.5.1.6. Maintaining a Bandwidth Utilization Chart

5.5.1.7. Providing Demand Management representation and information to the CAWG.

6. Service Design. Service Design identifies service requirements and devises new service offerings as well as changes and improvements to existing ones. Service Catalog Management, Service Level Management, Availability Management, Capacity Management, Service Continuity Management, Information Security Management, and Supplier Management make up USAFA's Service Design Process.

6.1. Service Catalog Management. Service Catalog Management ensures that a USAFA IT Service Catalog is produced, maintained and contains accurate information on all operational services. The USAFA IT Service Catalog provides vital information for all Service Management processes.

6.1.1. The USAFA IT Service Catalog will be maintained as current and will be available to USAFA customers on SharePoint.

6.1.2. The USAFA IT Service Catalog will contain all items as listed on Attachment 2 and accurately represent all USAFA C&I services.

6.2. Service Level Management. Service Level Management is the process for ensuring that all operational level agreements and underpinning contracts are appropriate and current. Service Level Management allows for the negotiation of Service Level Agreements (SLA) with customers and design of services in accordance with the agreed service level targets.

6.2.1. 10 CS and PMs develop and maintain SLAs for the systems under their purview IAW the USAFA IT Enterprise Schema. Each SLA shall at a minimum:

6.2.1.1. Identify key stakeholders.

6.2.1.2. Define minimum levels of service associated with each IT service.

6.2.1.3. Define prioritization of services and service restoration based upon mission requirements.

6.2.1.4. Define prioritization of user requests based upon mission requirements.

6.2.1.5. Define capacity requirements.

6.2.1.6. Define service availability requirements.

6.2.1.7. Define demand expectations, include the identification of cyclical demand requirements and any black out requirements (no system changes).

6.2.1.8. Define customer support requirements and hours of operation.

6.3. Availability Management.

6.3.1. Availability Management defines, analyzes, plans, measures and improves all aspects of the availability of IT services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, bandwidth, and roles are appropriate for the agreed availability targets. System PMs are responsible for the availability management of systems under their purview IAW the USAFA IT Enterprise Schema.

6.4. Capacity Management.

6.4.1. Capacity Management ensures that the capacity of IT services and the IT infrastructure delivers the agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service and plans for short, medium and long term business requirements. System PMs are responsible for the capacity management of systems under their purview IAW the USAFA Enterprise IT Schema.

6.5. Service Continuity Management.

6.5.1. IT Service Continuity Management plans for the provision of minimum service levels during natural disasters or other service disruptions. System PMs are responsible for the IT service continuity management of systems under their purview IAW the USAFA IT Enterprise Schema.

6.6. Information Security Management.

6.6.1. Information Security Management ensures confidentiality, integrity and availability of an organization's information, data and IT services. Information Security processes are addressed within the Access Management function in paragraph 8.7. and within the USAFA IT Enterprise VMP.

6.6.2. The USAFA IT Enterprise VMP is a compilation of all Core System VMPs.

6.6.3. Core System PMs develop their VMP to contain processes that address information security and contain at a minimum the following:

6.6.3.1. Vulnerability management reporting and compliance requirements to include a reporting matrix for the system.

6.6.3.2. Detailed monthly metric requirements for vulnerability management compliance and situational awareness for items such as Cyber Workforce Training compliance, Federal Information Security Management Act compliance, STIG Compliance, Host-Based Security System (HBSS) results, Penetration Attempts, and numbers of Category I, II, III and IV vulnerabilities.

6.7. Acquisition Process/Supplier Management.

6.7.1. Supplier Management ensures that all contracts with suppliers support the needs of the organization and that all suppliers meet their contractual commitments. Supplier management is operated IAW AFMAN 17-1203, AFMAN 63-144, *Defense Business System Life Cycle Managemen,t* and AFI 63-101/20-101, *Integrated Life Cycle Management.*

6.7.2. IT assets (hardware and software) are procured through applicable AF IT procurement processes outlined in AFMAN 17-1203. USLMs assigned will assist the BSLM in the management of unit software assets IAW AFMAN 17-1203.

6.7.2.1. Technology Commodity Council (ITCC) enterprise buying programs such as AFWay, DOD Enterprise Software Initiative (DOD ESI) or NETCENTS-2.

6.7.2.2. NETCENTS-2 contracts are accessed through AFWay at **https://www.afway.af.mil**.

6.7.2.2.1. Each unit will ensure that their Unit IT Property Manager has established a work flow IAW the AFWay User Manual prior to beginning the request for quote or ordering process.

6.7.2.3. The DOD ESI can be accessed at **http://www.esi.mil**.

6.7.2.4. Any exceptions to the use of required AF purchasing programs or asset standard configurations must have an approved exception obtained during the IT Change Management Process and/or the AFWay waiver process.

6.7.2.5. IT purchases must be planned for and executed in the proper PEC, EEIC and/or Object Class. Planning and execution items must match information investment information recorded in ITIP.

7. Service Transition.

7.1. Service Transition builds and deploys new or modified services IAW DESMF and ITIL. Transition Planning and Support, Change Management, Service Validation and Testing, A&A, Asset and Configuration Management, Release and Deployment Management, and Knowledge Management are processes under USAFA's Service Transition.

7.2. Transition Planning and Support

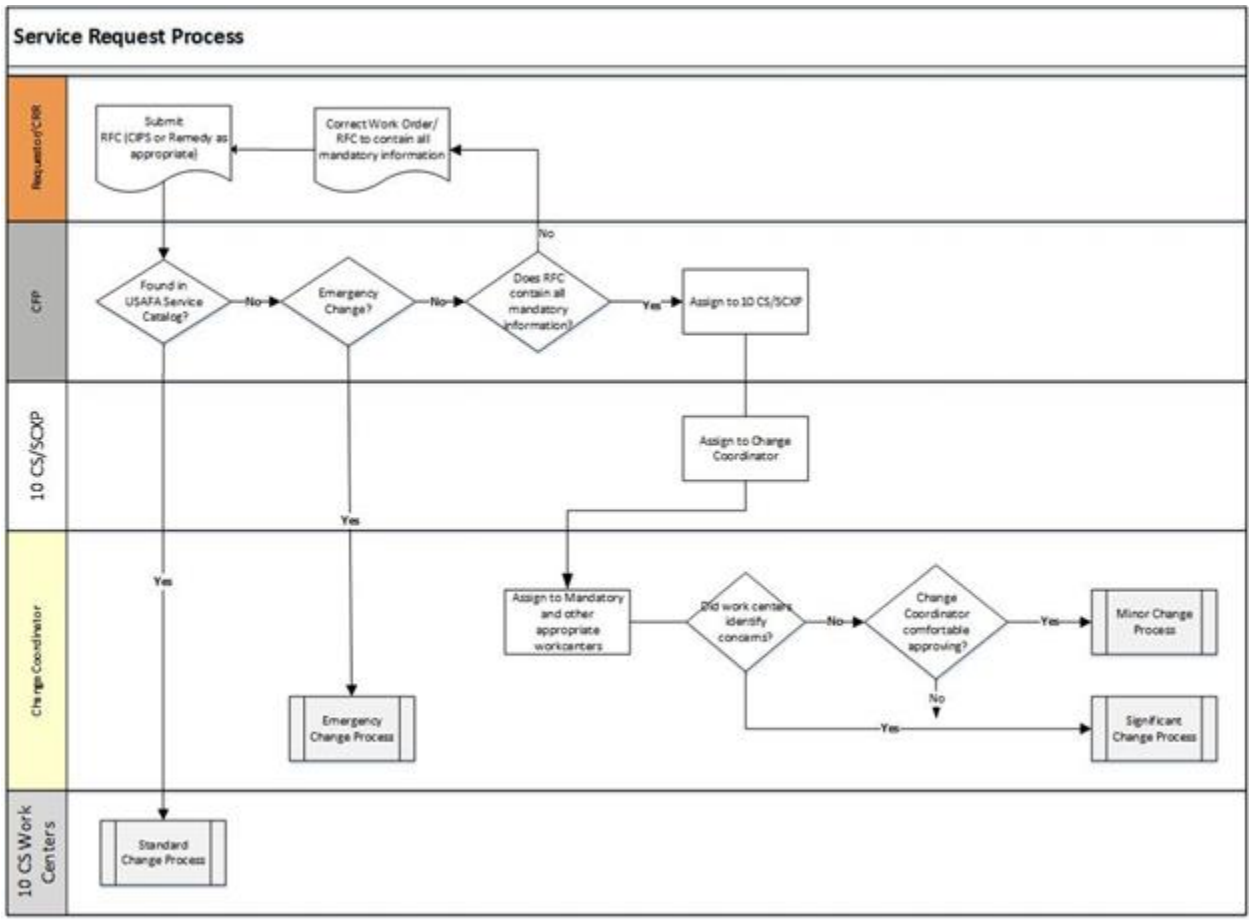
7.2.1. Transition planning and support aims to plan and coordinate the resources to deploy a Major Release within the predicted cost, time, and quality estimates. 10 CS PjMs and System PMs own this process and accomplish support IAW the Change Management and Release and Deployment Processes.

7.3. USAFA IT Change Management Process.

7.3.1. The IT Change Management is designed to help control the lifecycle of strategic, tactical and operational changes to IT services through standardized procedures. The primary objective of Change Management is to enable the initiation of beneficial Changes with minimum disruption to IT services. An ITChange is defined as any alteration, variation, Service Catalog exception, or modification to the USAFA IT Enterprise, any IT system, component of any system, Configuration Item (CI), or their associated peripherals, documents, and operation of the same. All IT service requests, IT hardware or software acquisition, IT configuration changes, requests for exception to IT policy must be approved IAW this IT Change Management Process prior to acquisition, installation, configuration change, operation, or implementation. The USAFA IT Change Management Process has five sub-processes: Service Request, Standard Change, Emergency Change, Minor Change and Significant Change. These processes are described below.

7.3.1.1. Service Request Process. Service Request is the process for handling and implementing requests for new and changed IT services, assets, documentation, and any requests for exception to the service catalog.

Figure 5. Service Request Process.



7.3.1.1.1. All new IT assets or services, IT change requests, IT service change requests, configuration changes, and requests for exception to IT policy or standards are submitted in CIPS. If the customer believes the request is already in the USAFA IT Service Catalog, they may contact the CFP to confirm submission vehicle (CIPS/Remedy).

7.3.1.1.2. All Work Order/RFCs must include the following elements prior to submission:

7.3.1.1.2.1. Note in request of owning ME, Director or PM validation or approval.

7.3.1.1.2.2. Change Description (item, requestor info, date required).

7.3.1.1.2.3. Defined requirements and specifications.

7.3.1.1.2.4. Suggested solution (optional).

7.3.1.1.2.5. Information on how unit is meeting this requirement today.

7.3.1.1.2.6. Justification (includes urgency and impact, justification for urgency and impact, risk if change not implemented, activity the RFC or requirement shall support).

7.3.1.1.2.7. Asset appropriation to include availability and source of funding (Funded, Unfunded, Endowment, AFAAC).

7.3.1.1.2.8. Configuration Management (details about CIs that are modified as part of change).

7.3.1.1.2.9. USAFA Form 136, *Software Request Questionnaire,* if a software request.

7.3.1.1.2.10. A signed USAFA Form 142, *USAFA Commercial ISP Agreement,* and draft waiver letter if a Commercial ISP request.

7.3.1.1.3. The CFP will review all Work Orders/RFCs to determine whether they are contained in the USAFA IT Service Catalog or qualify as an Emergency Change.

7.3.1.1.4. If the request is in the USAFA IT Service Catalog the CFP will assign the Work Order/RFC to the appropriate work center to begin the Standard Change Process in paragraph 7.3.1.2.

7.3.1.1.5. If the Work Orders/RFC is an Emergency Change, the CFP will assign the Work Order/RFC to the Change Coordinator to begin the Emergency Change Process in paragraph 7.3.1.3.

7.3.1.1.6. If the request is not in the USAFA IT Service Catalog or an Emergency Change the CFP will review the Work Order/RFC to ensure all information is included IAW paragraph number 7.3.1.1.2.

7.3.1.1.7. If information is missing the CFP will return the Work Order/RFC to the CRO for corrections.

7.3.1.1.8. Once all information is verified; the CFP will assign the Work Order/RFC to 10 CS Plans and Programs (10 CS/SCXP). 10 CS/SCXP will assign the Work Order/RFC to the Change Coordinator.

7.3.1.1.9. Change Coordinator will assign to the following mandatory work centers for review.

7.3.1.1.9.1. USAFA Cybersecurity Office

7.3.1.1.9.2. USAFA Portfolio Manager

7.3.1.1.9.3. USAFA Privacy Office/Records

7.3.1.1.9.4. The Change Coordinator will determine if the Work Order/RFC should be reviewed by other work centers and assign as appropriate. All CIPS work centers will be considered.

7.3.1.1.10. If the Work Order/RFC is coordinated with no concerns from the above workflows, and the Change Coordinator determines that the change does not require higher-level decision, then the Change Coordinator will assign to the appropriate work center to begin the Minor Change Process in paragraph 7.3.1.4.

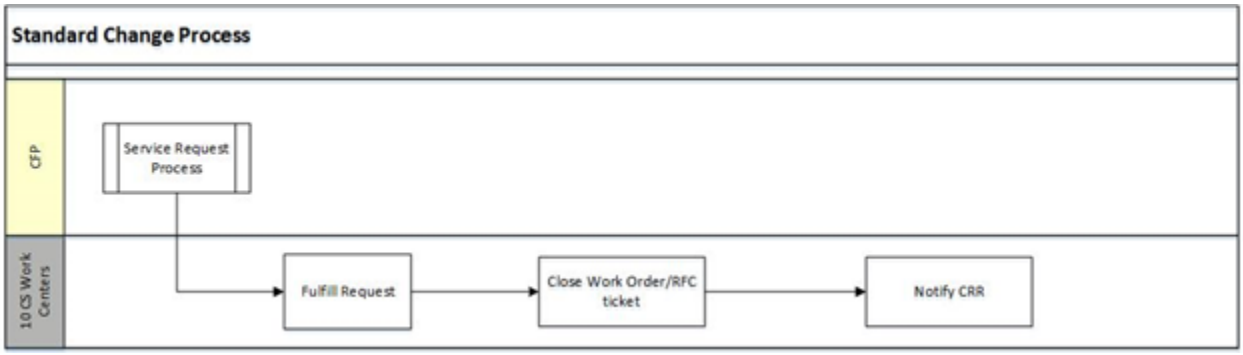
7.3.1.1.11. If the Work Order/RFC is coordinated with concerns from the above work centers, or if the Change Coordinator determines that the change requires higher-level decision, then the Change Coordinator will assign to the appropriate work center to begin the Significant Change Process in paragraph 7.3.1.5.

7.3.1.1.11.1. Work Order/RFCs with significant deviation from the current configuration, cybersecurity issues, a change to an ATO package, impacts to other system/services, all unfunded requirements, endowed IT assets/systems/services, and all exceptions to policy and waivers will be considered Significant Changes.

7.3.1.2. Standard Change Process

7.3.1.2.1. Standard Changes are preapproved, repetitive, low-risk, well-tested changes (e.g. new accounts, telephone changes/additions, email, small hardware, and standard software/system access requests). These actions are found in the USAFA IT Service Catalog.

Figure 6. Standard Change Process.



7.3.1.2.2. If the request is in the USAFA IT Service Catalog, the CFP will assign the CIPS work order to the appropriate work centers.

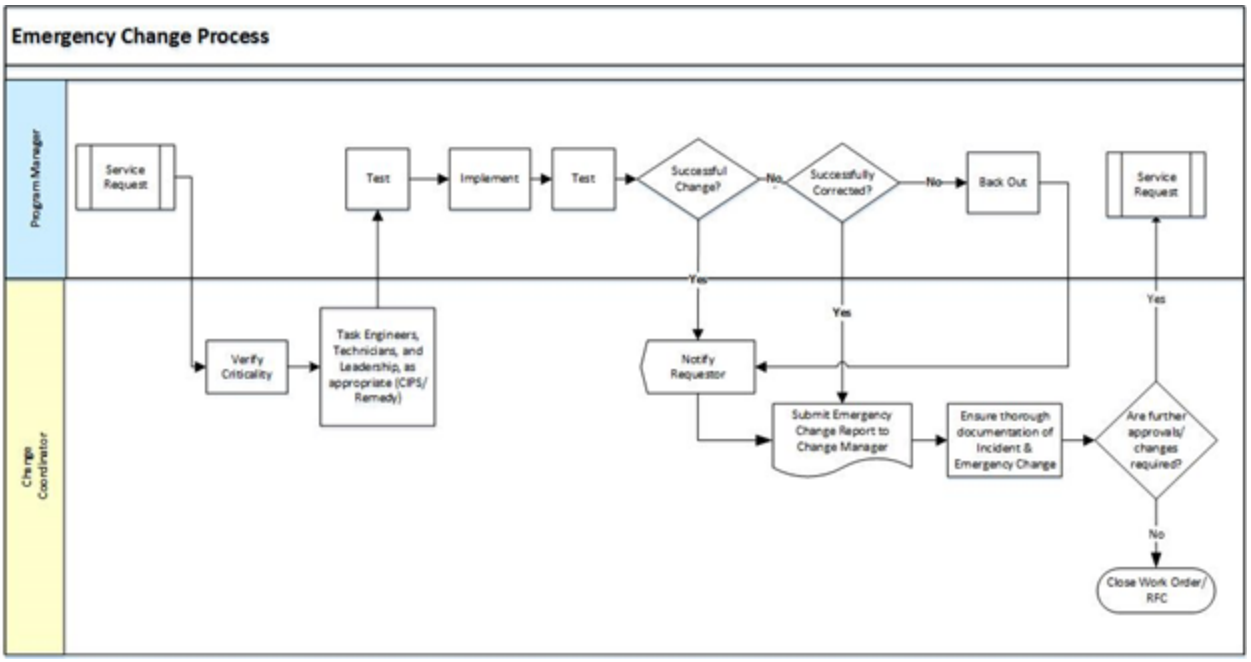
7.3.1.2.3. The work centers will fulfill their tasks, close their tasks in CIPs or Remedy and notify the CRO that the task has been completed.

7.3.1.2.4. Candidates for Standard Change designation must first go through the complete Significant Change process and take on the Standard Change designation only after CAWG review and approval. The Change shall then be added to the USAFA IT Service Catalog. Subsequent submissions will then be eligible for processing as a Standard Change.

7.3.1.3. Emergency Change Process.

7.3.1.3.1. Emergency Change is a change requiring immediate implementation to correct a Major Incident, security patch, or Problem. Emergency changes require the approval of the 10 CS Director (or equivalent) to be implemented.

Figure 7. Emergency Change Process.



7.3.1.3.2. The Change Coordinator shall verify the criticality of the emergency and notify the 10 CS leadership, appropriate engineers, technicians, and any other appropriate work center. The action work centers will be tasked in Remedy or CIPS as appropriate.

7.3.1.3.3. The system PM shall test the solution, as much as possible, prior to implementation to verify a clean solution.

7.3.1.3.4. The system PM shall implement the RFC correction as required.

7.3.1.3.5. The system PM shall test the implementation to validate correction of the emergency and the clearance of complications.

7.3.1.3.6. If the change was successful the Change Coordinator shall notify the requestor of success, document in the Monthly Change Report, ensure proper documentation of change and determine if further approvals or changes are required.

7.3.1.3.7. If the change was not successful the system PM shall attempt addition solutions until it is necessary to back out of any changes. The requestor shall be notify of unsuccessful correction.

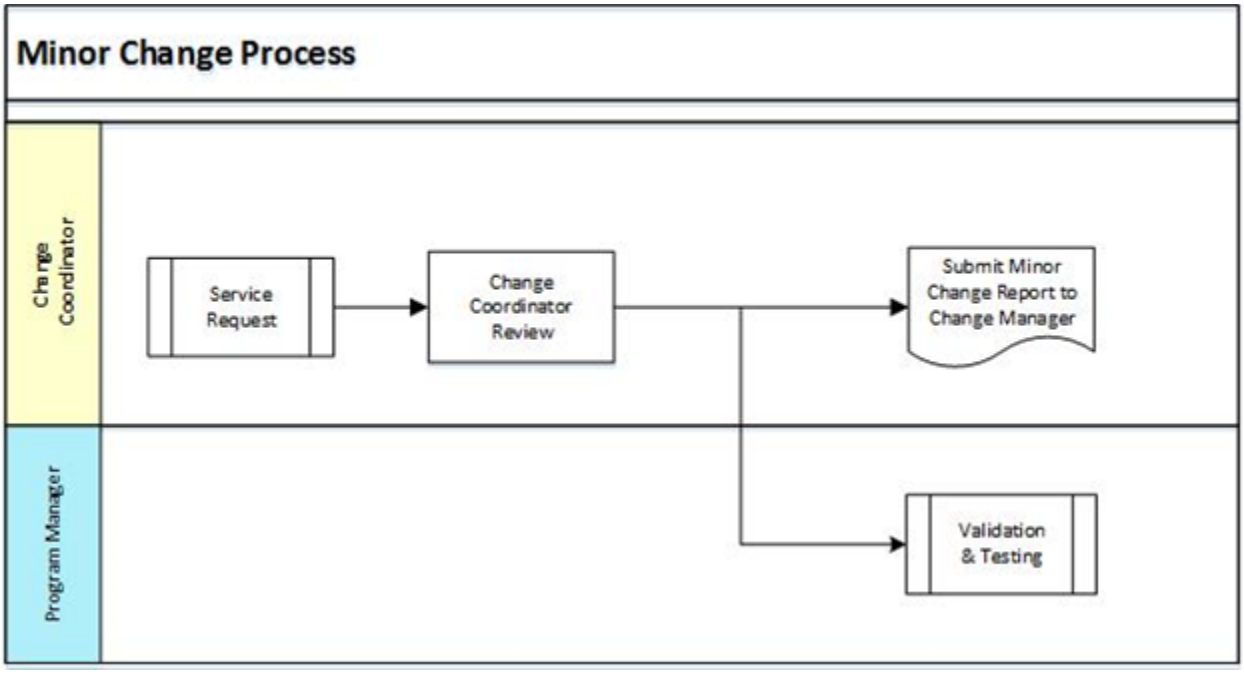
7.3.1.3.8. If further changes are required the Change Coordinator will notify the system PM to submit a Work Order/RFC to process the additional changes IAW the IT Change Management Process.

7.3.1.3.9. If no additional changes are required the Change Coordinator will close the Work Order/RFC.

7.3.1.4. Minor Change Process

7.3.1.4.1. Minor Changes have low, up to average risk, are well-understood changes with no serious configuration, service interruptions, demand, capacity or SLA violations expected.

Figure 8. Minor Change Process.



7.3.1.4.2. The Change Coordinator will review Minor Changes to validate the requirement and determine level of risk.

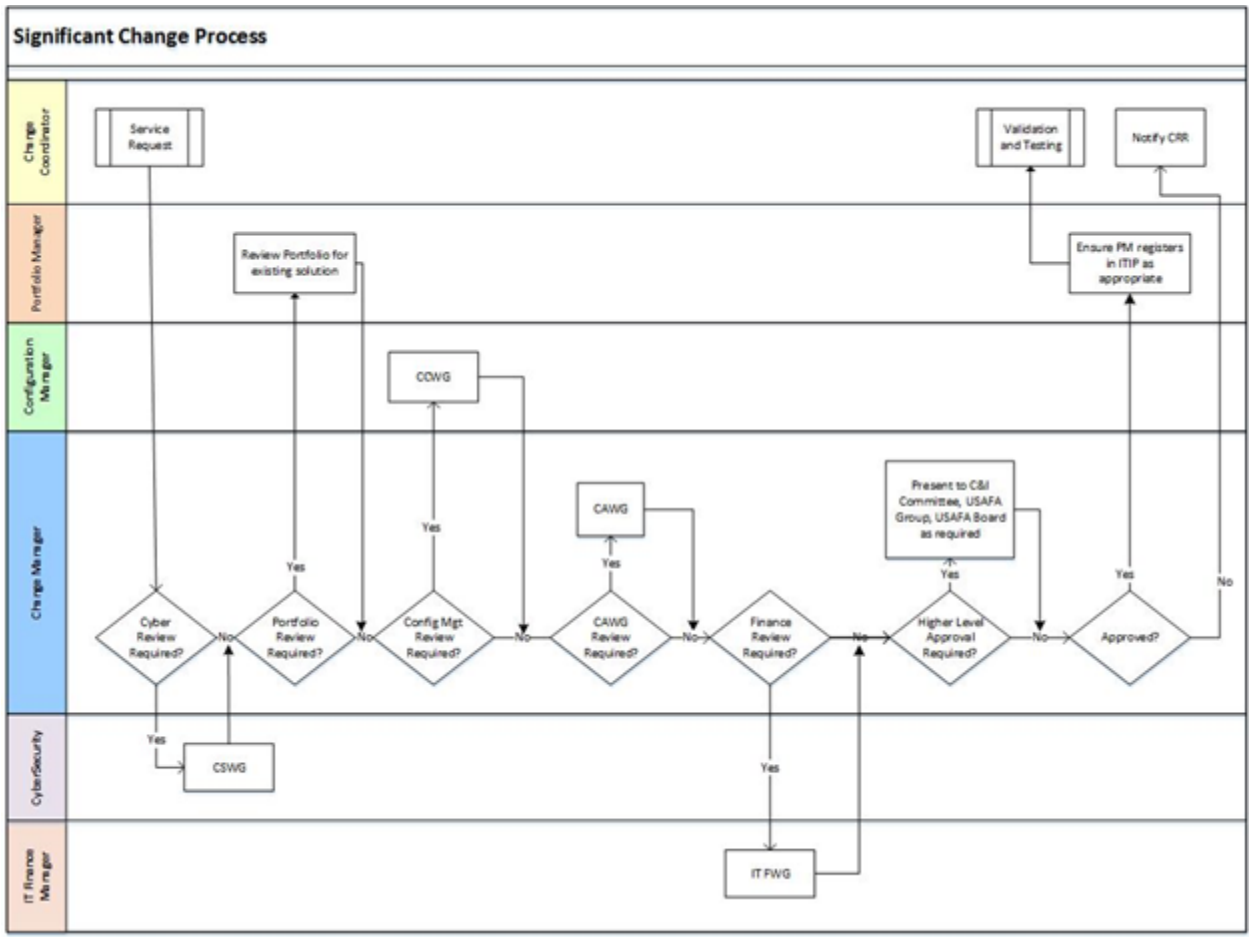
7.3.1.4.3. The Change Coordinator will notify the PM to start the Service Validation and Testing Process.

7.3.1.4.4. The Change Coordinator will consolidate all approved minor changes into the Monthly Change Report and send to the Change Manager.

7.3.1.5. Significant Change Process.

7.3.1.5.1. Significant Changes involve a significant amount of evaluation, planning, preparation, expense, service disruptions, impact to other services or risks to security. A significant change also represents significant deviation from current configuration, cybersecurity issues, a change to an ATO package, concerns identified during Service Request workflows, all unfunded requirements, endowment IT assets/systems/services, and all exceptions to policy and waivers.

Figure 9. Significant Change Process.



7.3.1.5.2. The Change Coordinator shall assign the Work Order/RFC to the Change Manager to begin the Significant Change process.

7.3.1.5.3. The Change Manager will review the RFC for cybersecurity concerns. If concerns exist the Change Manager will assign RFC to the USAFA Cybersecurity Office.

7.3.1.5.4. The ISSM shall conduct a CSWG as applicable and report results to the Change Manager.

7.3.1.5.5. Once the CSWG results are received or if there were no Cybersecurity concerns, the Change Manager will assign the RFC to the USAFA Portfolio Manager.

7.3.1.5.6. The USAFA Portfolio Manager will review the USAFA Portfolio for an existing solution/asset and report results to the Change Manager.

7.3.1.5.7. Once the portfolio review results are received; the Change Manager will review the RFC for configuration concerns. If concerns exist the Change Manager will assign the RFC to the Configuration Manager.

7.3.1.5.8. The Configuration Manager will conduct a CCWG if necessary and report back to the Change Manager.

7.3.1.5.9. Once the CCWG results are received or if there were no configuration concerns; the Change Manager will review the RFC for change concerns.

7.3.1.5.10. If there are change concerns the Change Manager will conduct a CAWG.

7.3.1.5.11. Once the CAWG results are received or if there were no change concerns; the Change Manager will review the RFC for financial concerns.

7.3.1.5.12. If there are financial concerns the Change Manager will assign the RFC to the IT Finance Manager.

7.3.1.5.13. The IT Finance Manager will review the RFC and determine if an ITFWG review is required. The IT Financial Manager will report back results of review or ITFWG to the Change Manager.

7.3.1.5.14. Once the IT Financial Manager results are received or if there were no financial concerns; the Change Manager will review the RFC for appropriate higher level approval requirement.

7.3.1.5.15. If higher level approval is required the Change Manager will present the RFC to the C&I Committee, USAFA Group or USAFA Board as required.

7.3.1.5.16. Once the higher level approval is received or if higher level approval was not needed the Change Manager shall assign the RFC to the:

7.3.1.5.16.1. Portfolio Manager who will ensure the PM enters the RFC into ITIP

7.3.1.5.16.2. Change Coordinator who will coordinate the RFC into the Validation and Testing process.

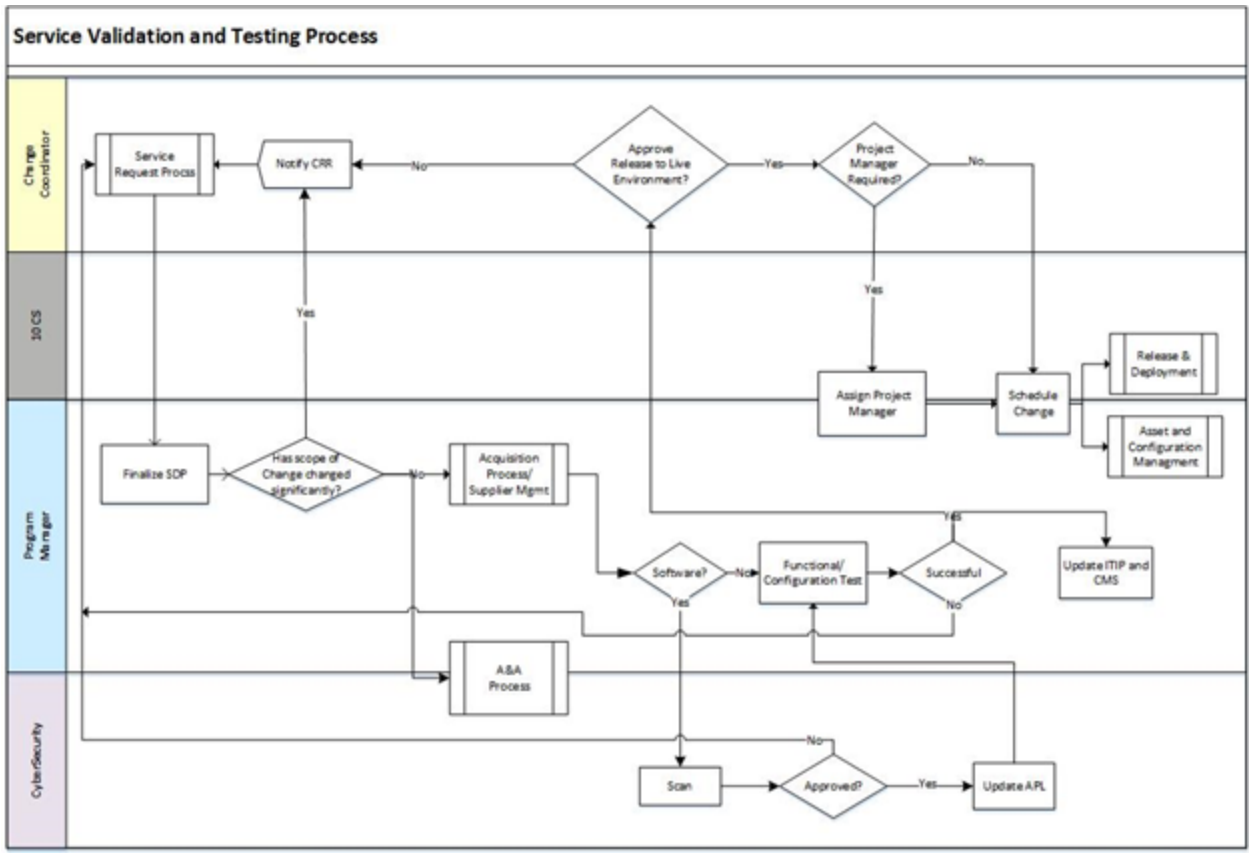
7.3.1.5.16.3. Notify the CRO.

7.3.1.5.17. If the RFC was not approved the Change Coordinator shall inform the requesting CRO of the approval decision and close the request.

7.4. Service Validation and Testing and Acquisition Process

7.4.1. Validation and Testing ensures that deployed releases and the resulting services meet customer expectations and is fit for purpose and use. Service Validation and Testing also verifies that IT operations are able to support the new service. Inefficient testing could cause a rise in Incidents and Problems.

Figure 10. Validation and Testing Process.



7.4.2. The PM finalizes the SDP and RFC to address any issues and formats as outlined in Attachment 3.

7.4.3. If it is determined that the scope of the RFC has changed significantly the RFC will be returned to the Change Coordinator for review and if necessary restart of the Service Request Process.

7.4.4. If the scope has not changed then the PM will start the Acquisition Process utilizing Supplier Management guidelines outlined in paragraph 6.7.

7.4.5. The PM will also work with the Cybersecurity office to start the A&A process in parallel with the Acquisition Process.

7.4.6. If the acquired asset is software the PM shall provide the USAFA Cybersecurity Office and the Base Software License Manager (BSLM) any purchased software for security scanning.

7.4.6.1. The USAFA Cybersecurity Office shall scan all new software for risks and the BSLM shall run virus scans and collect and track licensing.

7.4.6.2. If the software passes all scans the USAFA Cybersecurity Office shall add the software to the ASL and return the software to the PM for functional/configuration testing.

7.4.6.3. If the software does not pass scans the USAFA Cybersecurity office shall notify the Change Coordinator and PM.

7.4.6.4. If the CRO chooses to resubmit the Service Request for different software, the Change Coordinator shall return the RFC to the CRO to change the requirement. The RFC will return to the Service Request Process.

7.4.7. If the acquired asset is not software the PM shall start functional/configuration testing.

7.4.8. The PM shall test the acquired asset by:

7.4.8.1. Establishing a test plan describing the activities and tasks required to roll out the release in different environments (Test and Live).

7.4.8.2. Test 'pass/fail' criteria in the test environment.

7.4.8.3. Document test results in the RFC package in CIPs.

7.4.8.4. Reset the test environment to a known state before/after testing.

7.4.9. If the RFC solution does not pass the pre-implementation testing the PM notify the Change Coordinator and CRO and restart the Service Request Process.

7.4.10. If the RFC solution passed the pre-implementation testing the PM will update ITIP and the CMS.

7.4.11. The Change Coordinator reviews the RFC and determines if it is approved to release to the live environment. If not approved the RFC is returned to the CRO.

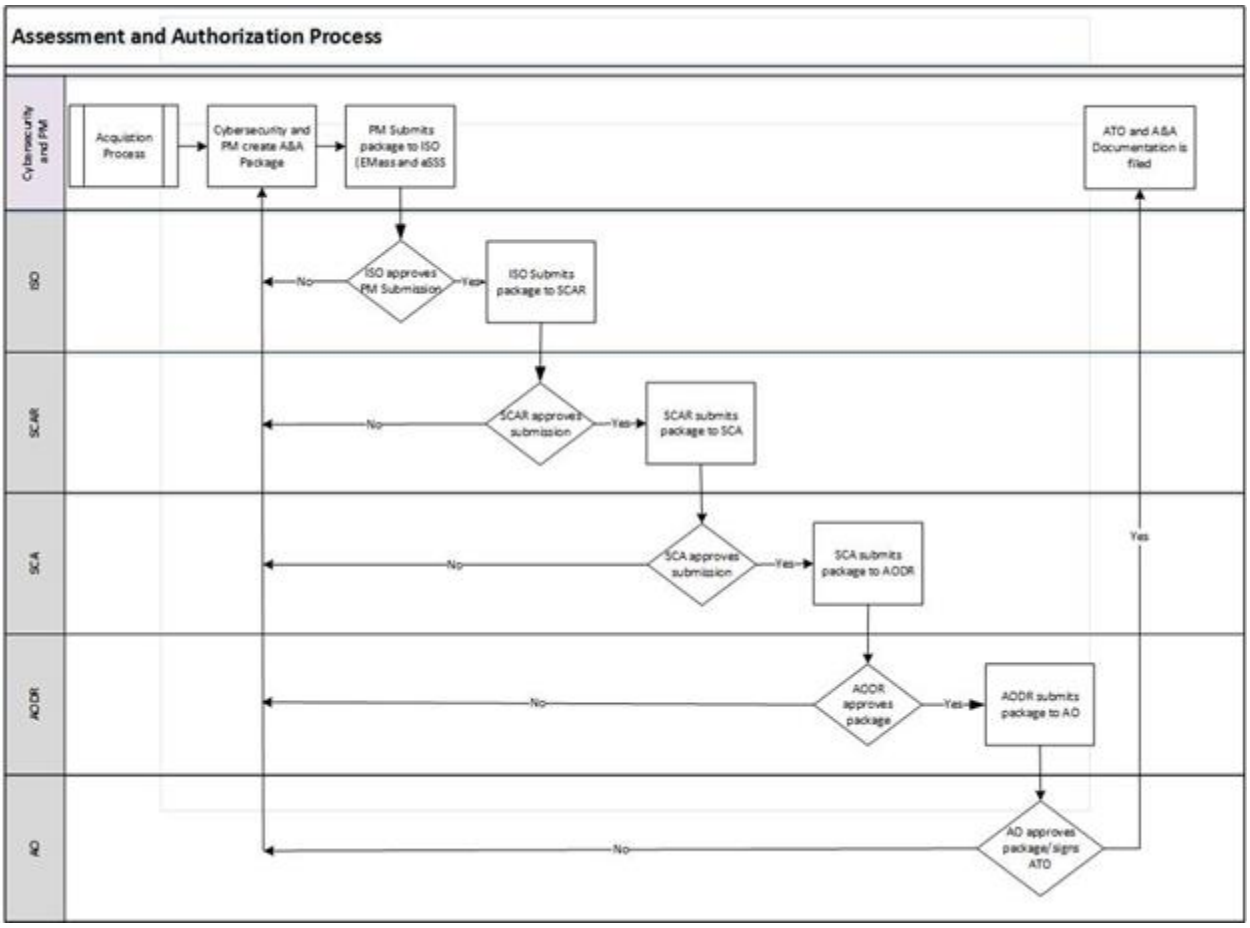
7.4.12. If the RFC is approved the change coordinator determines whether a PjM is required. If it is determined that a PjM is required, 10 CS and the PM will work together to assign a PjM.

7.4.13. The PM (and PjM if assigned) continues the Acquisition Process utilizing Supplier Management guidelines outlined in paragraph 6.7, schedules the RFC, begins Asset and Configuration Management as outlined in paragraph 7.6 and enters the Release & Deployment Process. The PM will work with the Change Coordinator to schedule the RFC and ensure that critical events in the USAFA Mission are identified (e.g., finals, in-processing, etc.) and IT change freeze periods do not conflict with the change scheduling.

7.5. Assessment and Authorization Process (A&A)

7.5.1. The A&A package is a living document and will be continually updated to capture new hardware, software, network diagrams, and cybersecurity controls. If a CAT I is introduced to the system that cannot be mitigated, the assessment package will be resubmitted to SAF CIO (via the AO) for approval. The SAF CIO can only grant a 6 month Interim Approval To Operate (IATO), and the CAT I must be mitigated and/or closed within the 6 months allowed by the IATO approval.

Figure 11. Assessment and Authorization Process.



7.5.2. The PM and USAFA Cybersecurity Office shall complete the A&A actions IAW AFI 17-101.

7.5.3. Approved exceptions and variances shall be included as artifacts in the applicable ATO package in eMass.

7.5.4. Cybersecurity and the PM initiate a A&A package in EMass and a eSSS package.

7.5.5. The PM submits the complete package to the ISO for approval. If approved the package is forwarded to the SCAR. If not approved the package is returned to the PM.

7.5.6. The SCAR approves the submission and forwards to the SCA. If not approved the package is returned to the PM.

7.5.7. The SCA approves the submission and forwards to the AODR. If not approved the package is returned to the PM.

7.5.8. The AODR approves the package and forwards it to the AO. If not approved the package is returned to the PM.

7.5.9. The AO approves the package and signs the ATO. The final package is returned to the PM and Cybersecurity for documentation and filing.

7.5.10. Once the A&A process is completed, the PM and USAFA Cybersecurity Office will notify the Change Coordinator.

7.5.11. The Change Coordinator shall review all RFC documentation and determine if the RFC solution is approved to release to the live environment.

7.5.12. If the RFC is not approved for release the Change Coordinator will notify the CRO to restart the Service Request Process.

7.5.13. If approved for release, the Change Coordinator shall notify the CRO the RFC is ready for deployment.

7.6. Asset and Configuration Management Process. Asset and Configuration Management helps to sustain network performance, reliability, and security, as well as enable cost savings through enterprise efficiencies. This process is responsible for identifying, controlling, recording, tracking, reporting, auditing and verifying the value and ownership of service assets throughout their lifecycles.

7.6.1. Asset Management is provided IAW AFMAN 17-1203 *Information Technology Asset Management*. LCR of USAFA assets is accomplished as a coordinated effort between 10 CS and PMs depending on funding source and USAFA IT Enterprise Schema level.

7.6.2. Configuration Management is provided as part of the change processes outlined in paragraph 7.3. The USAFA Configuration Manager and the CCWG reviews, validates and approves configuration changes. Configuration is controlled and tracked through a CMS.

7.6.2.1. The CMS is a repository for all USAFA CIs and is a section of the USAFA IT Service Catalog. It includes IT infrastructure data, IT architecture documentation and diagrams.

7.6.2.2. The CMS is considered a 'living document' and will be updated as frequently as required to maintain currency.

7.6.2.3. The CMS should be documented, maintained and available for review by the CCWG during the Significant Change Process.

7.6.2.4. No CI shall be added, modified, replaced, or removed without appropriate control documentation or change management procedure.

7.6.2.5. The CMS should have conformity between the documented baseline and the actual system referenced.

7.6.2.6. A system CMS will contain the following information:

7.6.2.6.1. Baseline Architecture or a description of the essential components of a service/system.

7.6.2.6.2. Configuration identification such as unique identifications, grouping, classification, characteristics and type.

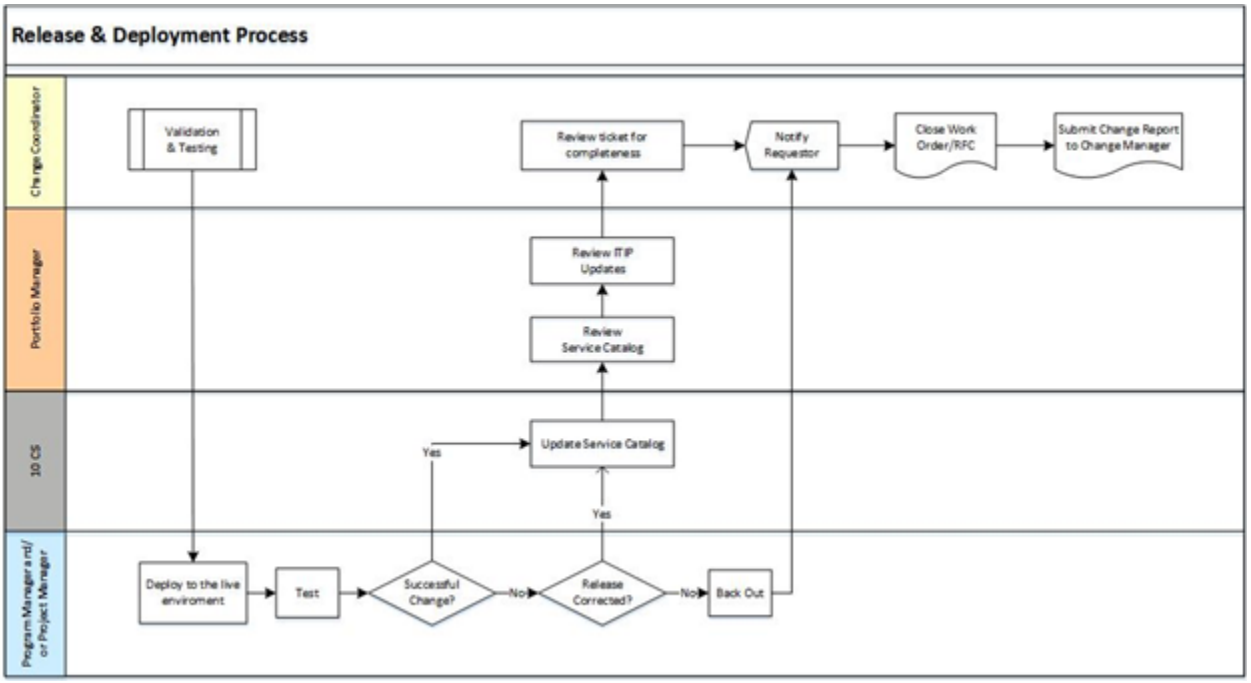
7.6.2.6.3. Relationships between CIs, assets, systems, applications and the USAFA IT Enterprise Architecture.

7.6.2.6.4. Logical models (diagrams), containing the components of the IT infrastructure (CIs) and their associations.

7.7. Release and Deployment Management Process

7.7.1. The primary objective of Release and Deployment Management is to plan, schedule and control the movement of releases to live environments. This ensures that the integrity of the live environment is protected and that the correct components are released without causing harm.

Figure 12. Release and Deployment Process.



7.7.2. The PM/PjM shall ensure that critical mission events are identified and that any IT change freeze periods do not conflict with deployment of the Change. The change schedule shall be coordinated between the Change Coordinator, PM, 10 CS and PjM as appropriate to deploy the Change to the live environment.

7.7.3. The PM/PjM shall deploy the change to the live environment and run the post deployment testing IAW the test plan outlined in paragraph 7.4.8.1.

7.7.4. If the test results are unsuccessful the PM/PjM will detect and remove functional and non-functional defects as soon as possible to reduce Incidents in the live environment.

7.7.5. The PM/PjM shall determine if release issues were corrected.

7.7.6. If corrections are not successful the PM/PjM will back out the release, document test results in the change package in CIPS, and notify the requestor.

7.7.7. If the test results in a successfully implemented Change then the PM/PjM will document the test results in the change package in CIPS and notify 10 CS.

7.7.8. 10 CS will update the USAFA IT Service Catalog and notify the USAFA Portfolio Manager.

7.7.9. The USAFA Portfolio Manager shall review the updates to the USAFA IT Service Catalog and ITIP.

7.7.10. The Change Coordinator shall review the RFC in CIPS for completeness, ensure that the deployed Change meets customer expectations and verify that IT operations are able to support the new service.

7.7.11. The Change Coordinator will close the Work Order/RFC when all Change actions are complete and include RFC update in the Monthly Change Report.

7.8. Knowledge Management

7.8.1. The objective of Knowledge Management is to gather, analyze, store and share knowledge and information within the organization and to improve efficiency by reducing the need to rediscover knowledge.

7.8.2. Knowledge Management includes SharePoint Administration, Shared Drive Administration, Privacy Act Program, Information Collections and FOIA Program and Records Management Program. These programs will be administered IAW DODD 5400.07 *DOD Freedom of Information Act (FOIA) Program,* DOD 5400.7-R_AFMAN 33-302 *Freedom of Information Act Program*, AFI 33-322 *Records Management Program,* AFI 33-324 *The AF Information Collections and Reports Management Program*, AFI 33-332, AFMAN 33-363, and AFI 33-396 *Knowledge Management.*

7.8.3. SharePoint Administration.

7.8.3.1. The 10 CS is responsible for SharePoint Administration. This process includes:

7.8.3.1.1. Creating accounts and assigning appropriate permissions for Site Collection Administrators (SPSCA).

7.8.3.1.2. Creating/managing and making available local SharePoint (SP) training for SPSCAs and Content Owners.

7.8.3.1.3. Supporting, operating, administering and maintaining all aspects of the day-to-day management of the SP server farm and its associated features, consulting services on tools available, troubleshooting, operating and maintaining the SP home page, reports and metrics.

7.8.3.1.4. Building custom SharePoint applications as requested through the Service Request Process.

7.8.4. Shared Drive Administration

7.8.4.1. The 10 CS is responsible for shared drive administration. The Shared Drive manager shall:

7.8.4.1.1. Comply with MPTO 00-33A-1113, *AFIN Server/Storage Management and Application Hosting* as appropriate.

7.8.4.1.2. Manage the USAFA network storage devices for organizational structure, content management and allocation limitations.

7.8.4.1.2.1. Allocation limitations are contained in the USAFA IT Service Catalog. Requests for changed to limitations will be requested utilizing the IT Change Management Process.

7.8.4.1.3. Scan for and notify PMs and units of unauthorized files or files not accessed/modified within the past 365 days.

7.8.4.1.4. Provide reports to PMs and units of files older than 5 years when requested. 10 CS may purge these files 30 days after notification if no exception is requested.

7.8.4.1.5. Ensure nightly backups of the shared drives and maintain a minimum of 60 days of backup for restoration purposes.

7.8.4.1.6. The following are specific Shared Drive requirements:

7.8.4.1.6.1. Official "O:" or Electronic Records Management drive is the network resource used to store official records.

7.8.4.1.6.1.1. USAFA has separate "O:" storage devices for the military and academic networks.

7.8.4.1.6.1.2. The directory structure is based on organization and office symbols that maintain official records IAW AFMAN 33-363.

7.8.4.1.6.1.3. Content Management is a responsibility of the Base Records Manager IAW AFI 33-364, Records Disposition. File retention is determined by the Air Force Records Disposition Schedule (RDS) located in AFRIMS on the Air Force Portal.

7.8.4.1.6.1.4. Access and permissions to the O:drive are managed by the Base Records Manager and are restricted by group permission levels. Requests for access are vetted through the unit Functional Area Records Manager (FARM). Vetted requests are then sent to the unit CSTs for .EDU and unit CLs for .MIL access.

7.8.4.1.6.1.5. Exceptions to data storage file types must be requested through the Base Records Manager.

7.8.4.1.6.2. Office-Restricted Organizational Data "N:" or ORG data drive is the network resource provided to share unit-specific information.

7.8.4.1.6.2.1. USAFA has separate "N:" storage devices for the military and academic networks.

7.8.4.1.6.2.2. The primary directory structure is based on organization and office symbols with other folders established as needed by organizations. Content management is the responsibility of applicable unit. Units may use the "N:" drive to maintain working or reference files that only pertain to the organization.

7.8.4.1.6.2.3. Access to the "N:" drive is limited to members assigned to that specific organization. Access and permissions to the "N:"drive are managed by the applicable unit. Requests for access are sent to the unit CSTs for .EDU and unit CLs for .MIL access.

7.8.4.1.6.2.4. Exceptions to data storage file types must be requested through the IT Change Management Process.

7.8.4.1.6.3. Cadet data "K:" or Cadet data drive is the network resource provided to share cadet specific information.

7.8.4.1.6.3.1. USAFA maintains a "K:" storage device only on the academic network.

7.8.4.1.6.3.2. Access to the "K:" drive is limited to members assigned to the Academic network. Access and permissions to the "K:" drive are managed by the applicable unit. Requests for access are sent to the unit CSTs.

7.8.4.1.6.3.3. Exceptions to data storage file types must be requested through the IT Change Management Process.

7.8.4.1.6.4. Applications "M:" or Applications drive is the central repository for all installation files, drivers, and supporting files such as installation instructions.

7.8.4.1.6.4.1. USAFA has separate "M:" storage devices for the military and academic networks.

7.8.4.1.6.4.2. This is the only location where executable files or software installs of any kind may be stored.

7.8.4.1.6.4.3. Access to the "M:" drive is maintained by 10 CS. Requests for access are sent to the CFP.

7.8.4.1.6.4.4. Exceptions to data storage file types must be requested through the IT Change Management Process.

7.8.4.1.6.5. Media "T:" or Media Drive is the central repository for all installation picture, video, image files.

7.8.4.1.6.5.1. USAFA maintains a "T:" storage device only on the academic network.

7.8.4.1.6.5.2. Access and permissions to the "T:" drive are managed by the applicable unit. Requests for access are sent to the unit CST.

7.8.4.1.6.5.3. Exceptions to data storage file types must be requested through the IT Change Management Process.

7.8.4.1.6.6. Database "X:" or database drive is solely used for various databases that are executed within the Academic domain.

7.8.4.1.6.6.1. USAFA has separate "X:" storage devices for the military and academic networks.

7.8.4.1.6.6.2. This is the only location where database files may be stored

7.8.4.1.6.6.3. Access to the "X ;" drive is maintained by 10 CS. Requests for access are sent to the CFP.

7.8.4.1.6.6.4. Exceptions to data storage file types must be requested through the IT Change Management Process.

7.8.4.1.6.7. Database "V:" or DF_Dept share drive is the network resource provided for academic class and research content.

7.8.4.1.6.7.1. Content Management and folder structure is controlled by HQ USAFA/DF.

7.8.4.1.6.7.2. USAFA maintains a "V:" storage device only on the academic network.

7.8.4.1.6.7.3. Access to the "V:" drive is limited to members assigned to the Academic network. Access and permissions to the "V:" drive are managed by HQ USAFA/DF utilizing permission groups. Requests for access are sent to the unit CSTs.

7.8.4.1.7. Privacy Act, PII, Personal Health Information (PHI) and Confidential Data, Health Insurance Portability and Accountability Act (HIPPA) or other sensitive information stored on shared drives must be protected within folders or by document passwords. Access to these files will be limited only to individuals whose official duties provide them with a valid need to know. Access to this sensitive data will be maintained IAW AFI 33-332.

7.8.4.1.8. Permissions to a file structure are granted via Distribution List security groups or standard security groups as appropriate. Permissions to Change, Write, Modify, and Delete on shared drive files are only granted to individuals with full access.

7.8.4.1.9. Individuals will only have permissions to shared organizational folders for the office of record where the individual works or as approved by a specific folder owner.

7.8.4.1.10. Shared Drives may contain only the data described by the particular drive. In addition the following data files are prohibited on all shared drives.

7.8.4.1.10.1. Backups and archives of computer hard drives.

7.8.4.1.10.2. Backups of a user's working files, favorites, and other data (including *.pst files) made for the explicit purpose of computer replacement.

7.8.4.1.10.3. Duplicates of downloaded official publications, libraries, forms from official web sites.

7.8.4.1.10.4. Software installation files other than those hosted by 10 CS.

7.8.4.1.10.5. Personal data files to include any of the following types: *.wav, *.jpg, *.mp3, *.mpeg, *.avi, *.pst, *:tmp, *.exe, *.ost, *.oab, *.wmv, *.mov, *.tif, *.bin, *.iso, *.nrg, *.vob, *.m4a, *.dll, *.sys, *.ocx, *.vbx, *.vxd, *.drv, *.scr, *.cpl, *.gho, *.msc

8. Service Operations.

8.1. Service Operation consists of the tasks necessary for service continuation. The Service Desk Function, Application Management, IT Operations Control Function, Incident Management, Problem Management, Access Management and Event Management are all part of Service Operations.

8.2. Service Desk Function.

8.2.1. The Communications Focal Point (CFP) provides the function of the Service Desk as the entry point between system users and services. The CFP will function IAW MPTO 00-33A-1001 *General Support Activities Management Procedures and Practice Requirements as outlined in the contract performance work statement*. Some service desk functions may be assigned to other work centers as determined by 10 CS, SLA or PM.

8.3. Application Management.

8.3.1. Application Management shall support the lifecycle of applications (requirements, development, build, deployment, operation, optimization, and retirement) that enhance the ability to provide services in support of the mission. This covers any software/application/system, other than operating systems and firmware, which resides on USAFA IT Infrastructure. Application Management is part of Service Transition and is owned by system PMs and HQ USAFA/A6 IAW the USAFA Enterprise IT Schema.

8.4. IT Operations Control Function.

8.4.1. The role of IT Operations is to execute the ongoing activities and procedures required to manage and maintain the IT infrastructure at the agreed service levels.

8.4.2. The 10 CS/SCO and system PMs shall:

8.4.2.1. Comply with MPTO 00-33A-1106, *AFIN Network Management*, MPTO 00-33A-1202, AFIN *Account Management,* and AFI 17-201.

8.4.2.2. Ensure that all day-to-day operational activities are carried out in a timely and reliable way.

8.4.2.3. Ensure infrastructure and systems are maintained, upgraded, replaced and/or removed to support service continuity and meet the requirements in accordance with documented SLAs.

8.4.2.4. Execute tasks related to the operation of infrastructure components and applications. This includes job scheduling, backup and restore activities, print and output management, and routine maintenance.

8.4.2.5. Ensure the "USAFA .EDU Guest" wireless service complies with the DISA STIGs.

8.4.2.6. Verify and provide document to the USAFA Cybersecurity Office the implementation of all STIG requirements.

8.4.2.7. Restrict streaming video on USAFA educational or mission networks. The NIPRNet, USAFA .EDU, ResearchNet, and commercial mission networks shall not be utilized for streaming video (e.g., Netflix, Hulu, HBOGO).

8.4.2.8. Capture audit logs and provide discrepancy reports to the USAFA Cybersecurity Office for review at least weekly.

8.4.2.9. Enable port security IAW MPTO 00-33A-1106.

8.4.2.10. Comply with the DOD Ports, Protocols, and Services Management (PPSM). The DOD PPSM Registry Database is the only authoritative source for Ports, Protocols, and Services information. Exceptions must be approved IAW the IT Change Management Process.

8.4.2.11. Block internet sites based on category or specific site. A list of blocked sites will be maintained and available in the USAFA IT Service Catalog. Exceptions must be approved IAW the IT Change Management Process.

8.4.2.12. Establish user mailbox limits IAW established limitations in the USAFA IT Service Catalog. Exception requests will be made IAW the IT Change Management Process.

8.4.2.13. Manage email distribution lists and authorized users/distributors for lists under their purview. Distribution and security list membership will be managed by the list owning organization.

8.4.2.13.1. The first line of every e-mail using a mass distro list will include an approval statement [i.e., THIS DISTRIBUTION (A, O, P or USAFA_ALL MESSAGE APPROVED BY (name of commander, department head, or director)].

8.4.2.13.2. Dist A: This list is used for information intended for the direct attention of commanders, directors and department heads.

8.4.2.13.2.1. Authorized distributors are commanders, department heads, directors, or their designated representative. The CFP may act as a designated representative if specific email is approved for distribution by other authorized distributor.

8.4.2.13.2.2. Authorized receivers are all 2-letter and tenant organization mailboxes.

8.4.2.13.3. Dist O: This list is used for information intended for organizational action of information.

8.4.2.13.3.1. Authorized distributors are commanders, department heads, directors, section chiefs, base program managers. The CFP may act as a designated representative if specific email is approved for distribution by other authorized distributor.

8.4.2.13.3.2. Receivers: all organization mailboxes for distribution by mailbox monitors to appropriate persons within the organization.

8.4.2.13.3.3. When using this distribution, the line after the approval statement describes the target group for the message (e.g., PLEASE DISSEMINATE TO ALL RECORDS CUSTODIANS). Mailbox monitors shall forward the message appropriately.

8.4.2.13.4. Dist P: This list is used only for time-sensitive, urgent, and official business that requires the immediate attention of the vast majority of recipients. Unauthorized use includes retirement invites, office parties, farewells, fundraisers, and encrypted email.

8.4.2.13.4.1. Authorized distributors are USAFA Superintendent and Mission Element Directors or designated representative. The CFP may act as a designated representative if specific email is approved for distribution by other authorized distributor.

8.4.2.13.4.2. Receivers: all USAFA personnel except cadets and cadet candidates.

8.4.2.13.5. USAFA All: This list is used only for time-sensitive, urgent, and official business impacting all personnel; i.e., notices of road closures, weather-related restrictions or closures, pending disaster, or other topics of similar gravity. Encrypted emails are unauthorized for use.

8.4.2.13.5.1. Authorized distributors are USAFA Superintendent and Mission Element Directors or designated representative. The CFP may act as a designated representative if specific email is approved for distribution by other authorized distributor.

8.4.2.13.5.2. Receivers: Every network user including cadets and cadet candidates.

8.5. Incident Management

8.5.1. Incident Management is the process for handling all incidents in order to restore normal service operations to users as quickly as possible and minimize impact on the mission. An incident is defined as an unplanned interruption or reduction in the quality of an IT service.

8.5.2. USAFA AFNet and .EDU users shall report all Incidents to the CFP via Remedy/vESD/email/phone as appropriate or the unit CST. All cybersecurity incidents are reported to their organization CL as well IAW with AFI 17-203, AFMAN 17-1201, MPTO 00-33A-1112 and the USAFA CIRP.

8.5.2.1. The USAFAVA 33-201, *Network Incident Reporting Aid,* should be used to document initial cybersecurity incidents.

8.5.3. The USAFA Cybersecurity Office will develop an overall USAFA Incident Response Plan. All Core System PMs shall develop and maintain an incident management response plan for systems under their purview IAW the USAFA Enterprise IT Schema. The technical incident management process will include at a minimum (IAW AFI 17-203):

8.5.3.1. Process for monitoring of system to detect and react to incidents, intrusions, disruption of services or other unauthorized activities.

8.5.3.2. Process for assisting users in assessing the scope of unauthorized network activities and incidents.

8.5.3.3. Process for containment, and/or elimination of potential incidents once they have been identified.

8.5.3.4. Process for termination of network services and isolation of offending networks or system until an incident is resolved.

8.5.3.5. Process for determining and monitoring the stage of escalation for unresolved incidents.

8.5.3.6. Process for user notification and customer satisfaction monitoring.

8.5.3.7. Process for submission of follow-up RFC tickets for solutions to recurring incidents.

8.5.4. In addition to the technical incident management processes listed above, the system Incident Management Response Plan will include the following Cyber Incident processes:

8.5.4.1. Reporting Structure

8.5.4.2. Incident Definitions and Categories

8.5.4.3. Roles and Responsibilities

8.5.4.4. Training Process

8.5.4.5. Reporting and Documentation Process

8.5.4.6. Response Procedures

8.5.4.7. Response Timelines

8.5.4.8. Response Team Membership

8.5.4.9. Exercise Schedule (at least biannually)

8.5.5. System IRPs are part of the system A&A package and must be submitted to the USAFA Cybersecurity Office for review and approval.

8.6. Problem Management.

8.6.1. A problem is defined as the unknown cause of one or more incident(s). The primary goal of the Problem Management Process is to prevent problems and resulting incidents from occurring, eliminate recurring incidents, identify the root cause, and minimize the impact of unresolved incidents.

8.6.2. Core system PMs shall develop and maintain a Problem Management Process for systems under their purview IAW the USAFA IT Enterprise Schema. The problem management process should at a minimum:

8.6.2.1. Manage the lifecycle of all Problems and document resolutions.

8.6.2.2. Maintain information/documentation about Errors and Workarounds.

8.6.2.3. Incorporate procedures as published in MPTO 00-33A-1114, *AFIN Problem Management*, as appropriate.

8.6.2.4. Process for submission of follow-up RFC tickets for solutions to problems.

8.7. Access Management.

8.7.1. Access management grants authorized users the right to use a service while preventing access to non-authorized users.

8.7.2. AFNet access management is governed by MPTO 00-33B-5004, *Access Control for Information Systems*, MPTO 00-33D-2001, *AFNET Naming Conventions*, DODD 5205.07, *Special Access Program Policy*, AFI 16-1404, *AF Information Security Program* and AFMAN 17-1301. AFNet user account provisioning is coordinated by unit CLs.

8.7.3. Authorized users on the USAFA .EDU are identified as: All cadets and personnel assigned to HQ USAFA staff agencies, HQ USAFA/DF, HQ USAFA/CW, HQ USAFA/AD, and HQ USAFA/PL.

8.7.3.1. SharePoint users on the AFNet will be provisioned for access to the .EDU incident of SharePoint.

8.7.3.2. Requestors shall complete the requirements in Table 8.7.

8.7.3.3. The unit CL will submit completed requests and documents to the CFP.

8.7.4. Visiting faculty, staff, and others (with or without CAC) requesting USAFA .EDU network user accounts or access to the guest wireless due to interaction with the academic mission shall complete appropriate documentation requirements listed in Table 8.7.

8.7.4.1. The unit CL will submit completed requests and documents to the CFP.

8.7.4.2. Documentation for visiting users will include:

8.7.4.2.1. Justification outlining mission and academic interaction with cadets and HQ USAFA/DF, HQ USAFA/CW, HQ USAFA/AD, USAFA Admissions (HQ USAFA/RR) and HQ USAFA/PL faculty.

8.7.4.2.2. Level of account/access required (i.e. access to SharePoint, CAMIS, access to USAFA .EDU e-mail account only, or full network user access)

8.7.4.2.3. Date the account shall expire.

8.7.5. Foreign nationals (cadets, faculty, staff) requesting USAFA .EDU access for performance of assigned duties shall complete appropriate documentation requirements listed in Table 8.7.

8.7.5.1. The unit CL will submit completed requests and documents to the CFP.

8.7.5.2. Foreign Nationals must also complete required actions on the USAFA Cybersecurity Office Foreign National Accounts SharePoint site. A memorandum certifying justification and restriction levels signed by a G-Series Officer is required. The G-Series Officer may delegate this access documentation responsibility in writing.

8.7.5.3. The USAFA Cybersecurity Office shall revalidate foreign national access quarterly.

8.7.6. USAFA personnel with elevated network privileges are considered to be members of the Cybersecurity workforce and are required to attain and maintain appropriate Cybersecurity certifications IAW DOD 8570.01-M and AFMAN 17-1303.

8.7.6.1. Privileged Users (FSA, CST etc.) must obtain and maintain at least a DOD 8570.01-M IAT Category Level II certification and provide evidence of certification to the USAFA Cybersecurity Office prior to obtaining a privileged account.

8.7.6.2. Individuals serving in existing privileged user roles who are not certified IAW DOD 8570.01-M and AFMAN 17-1303, will have their privileges revoked immediately when discovered until they can provide evidence of certification.

8.7.6.3. Foreign National privileged users must meet DOD 8570.01-M and AFMAN 17-1303 requirements.

8.7.6.3.1. HQ USAFA/IP shall validate and the USAFA Cybersecurity Office shall approve support documentation and requests IAW AFMAN 17-1301, MPTO 00-33B-5004, and MPTO 00-33A-1301-WA-1, *Foreign National NIPRNET Access Core Service.*

Table 6. USAFA Access Requirements.

These requirements apply to NIPRNet, SIPRNet, CAMIS, and ResearchNet Core.					
	CAC User	Foreign National	Privileged User	SIPRNet User	Non-CAC Holder (Guest Net user)
DD2875 *System Authorization Access Request*	X	X (1)	X	X	NA
AF Form 4394 *AF User Agreement Statement*	X	X	X	X	NA
DOD Information Assurance Awareness (IAA) Cybersecurity Awareness Training Certification	X	X	X	X	NA
DD Form 2842 *DOD PKI Certificate of Acceptance and Acknowledgement of Responsibilities*				X	NA
Access MFR		X			NA
Appropriate Cybersecurity Workforce Training Certificate			X		NA
Work Order (Remedy ticket)	X	X	X	X	X
USAFA Form 75			X	X	
Note 1: Use appropriate template from Foreign National Account SharePoint site					

8.7.7. The USAFA .EDU Guest wireless is for official use only or for use during an official event. Authorized guests include (but are not limited to) distinguished visitors, foreign dignitaries, congress, senators, personnel on TDY, or local/state government employees. Unauthorized guests include (but are not limited to) cadet families, general public, retirees, Association of Graduates personnel (AOG).

8.7.7.1. 10 CS shall maintain a list of approved guests and approved expiration date.

8.7.7.2. Access is for government-owned, non-CAC authenticating devices.

8.7.7.3. Access shall be enabled only for the duration of the approved official event or official requirement.

8.7.8. Other Access Considerations.

8.7.8.1. Access processes for other than core systems will mirror the AFNet access process as appropriate. Access for these systems will be managed by the PM in coordination with HQ USAFA/IP and the USAFA Cybersecurity Office.

8.7.8.2. User profiles will be standardized across each core system.

8.7.8.2.1. Naming conventions are accomplished in IAW MPTO 00-33D-2001. The addition of education degrees or certification designations is acceptable.

8.7.8.3. User accounts will be locked, closed, or disabled IAW AFMAN 17-1301 and MPTO 00-33B-5004.

8.7.8.4. User accounts will be disabled after 30 days of inactivity unless extended absence is identified in advance (e.g., Deployment, Temporary Duty, etc.).

8.7.8.5. User accounts will be deleted 60 days after disabled.

8.7.8.6. User accounts will be locked immediately:

8.7.8.6.1. Upon personnel termination or resignation; the account will be deleted after 10 days.

8.7.8.6.2. Upon account holder identification as a security risk (i.e. lost clearance) IAW AFMAN 17-1301. The USAFA Cybersecurity Office has the authority to terminate the account.

8.7.8.7. User accounts that no longer require academic mission interaction will be deleted. Disable Cadet/Cadet Candidates accounts within 5 duty days after graduation (or drop) and delete after 30 days.

8.7.8.8. Lock accounts [regardless of security clearance] where Users were found to participate in conduct that is inconsistent with Cybersecurity policies and guidelines or Security violations IAW AFMAN 17-1301 and AFMAN 17-1201. These accounts shall remain locked until:

8.7.8.8.1. Commander is notified.

8.7.8.8.2. Cybersecurity training is re-accomplished by the violator

8.7.8.8.3. Both the violator's computer and the receiver's system (if necessary) is cleaned.

8.7.8.8.4. Memo for Record (MFR) is completed by the commander stating the violator has re-accomplished cybersecurity training and received by USAFA Cybersecurity.

8.7.8.9. Requests for interim administrative accounts are authorized for imaging of incoming cadet client systems. The organization CL will submit these requests. Interim Administrative Accounts shall:

8.7.8.9.1. Consist of individuals needed to image the incoming cadet laptops only.

8.7.8.9.2. Gain permissions using access password with an expiration date.

8.7.8.9.3. Expire after the approved set length of time.

8.7.9. Commercial Internet Service

8.7.9.1. Commercial Internet Services will be requested IAW with the IT Change Management Process. Requestor shall:

8.7.9.1.1. Submit a Work Order/RFC ticket via the organization CRO.

8.7.9.1.2. Ensure budgeting and funding for all initial and recurring charges necessary to maintain the services, including stand-alone computers.

8.7.9.1.3. Complete a signed USAFA 142, *USAFA Commercial ISP Agreement,* and draft a waiver request letter for validation. Contact the USAFA Cybersecurity Office for waiver letter samples.

8.7.9.1.4. Ensure no sensitive government data, PII, FOUO, or classified information is processed/ transmitted on the commercial ISP.

8.7.9.1.5. Ensure devices connecting to the commercial ISP:

8.7.9.1.5.1. Are sanitized prior to initial use to remove all official use only and/or sensitive but unclassified information.

8.7.9.1.5.2. Maintain physical and logical separation from the government network infrastructure.

8.7.9.1.5.3. Contain firewalls or approved antivirus software (e.g., McAfee or Norton Antivirus).

8.8. Event Management.

8.8.1. Event Management is the process that monitors all events occurring on the USAFA IT infrastructure, evaluates the impact of the event to USAFA services, and escalates exception conditions. Event Management ensures that CIs and services are constantly monitored, filtered and categorized in order to perform appropriate actions. An event is defined as any detectable or discernible occurrence that impacts IT infrastructure or the delivery of IT service. Events are typically discovered through notifications created by an IT service, CI, or monitoring tool. The Event Management process is owned by system PMs.

9. IT Continual Service Improvement .

9.1. System PMs will develop appropriate metrics to track critical success factors and key performance indicators that align with the USAFA IT Strategic Plan. Metrics will also be developed that monitor IT system performance and services.

9.2. ISOs and PMs will periodically review metrics for systems under their purview for improvement opportunities.

DAVID J. HLUSKA, GS-13, DAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

The Clinger-Cohen Act (CCA) -- Subtitle III of Title 40 United States Code

DODD 5205.07, *Special Access Program Policy*, 1 July 2010

DODD 5400.07, *DOD Freedom of Information Act (FOIA) Program*, 2 January 2008

DODD 8000.01, *Management of the DOD Information Enterprise*, 17 March 2016

DODD 8115.01, *Information Technology Portfolio Management*, 10 October 2005

DODD 8440.01, *Information Technology Service Management (ITSM)*, 24 December 2015

DODI 8500.01, *Cybersecurity*, 14 March 2014

DODI 8510.01, *Risk Management Framework for DOD Information Technology*, 12 March 2014

DOD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, 21 October 2010

DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

DOD PPSM Registry Database

The DOD Enterprise Service Management Framework (DESMF)

AFI 16-1404, *AF Information Security Program*, 29 May 2015

AFI 17-100, *Air Force Information Technology (IT) Service Management*, 16 September 2014

AFI 17-101, *Risk Management Framework (RMF) for AF Information Technology*, 2 February 2017

AFI 17-110, AF *Information Technology Portfolio Management and IT Investment*, 23 December 2008

AFI 17-130, *AF Cybersecurity Program Management*, 31 August 2015

AFI 17-201, *Command and Control (C2) for Cyberspace Operations*, 5 March 2014

AFI 33-322, *Records Management Program*, 4 June 2012

AFI 33-324, *The AF Information Collections and Reports Management Program*, 6 March 2013

AFI 33-332, *AF Privacy and Civil Liberties Program*, 12 January 2015

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 33-396, *Knowledge Management*, 7 November 2014

AFI 35-107, *Public Web Communications*, 21 October 2009

AFI 63-101/20-101, *Integrated Life Cycle Management*, 7 March 2013

AFMAN 17-1201, *User Responsibilities and Guidance for Information Systems*, 1 June 2012

AFMAN 17-1202, *Collaboration Services and Voice Systems Management*, 6 September 2012

AFMAN 17-1203, *Information Technology Asset Management*, 19 March 2014

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*, 1 November 2016

AFMAN 17-1402, *AF Clinger-Cohen Act (CCA) Compliance Guide*, 24 October 2012

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 33-402, *Service Development and Delivery Process (SDD*P), 25 September 2014

AFMAN 63-144, *Defense Business System Life Cycle Management*, 31 March 2016

USAFAVA 33-201, *Network Incident Reporting Aid*, 1 April 2016

MPTO 00-33A-1001, *General Support Activities Management Procedures and Practice Requirements*, 1 July 2016

MPTO 00-33A-1100, *AFNet Operations Change Management Process*, 2 December 2014

MPTO 00-33A-1106, *AFIN Network Management*, 12 June 2014

MPTO 00-33A-1109, *AFIN Vulnerability Management*, 5 November 2015

MPTO 00-33A-1112, *Air Force Network Enterprise Service Desk Service Incident Management*, 19 May 2014

MPTO 00-33A-1113, *AFIN Server/Storage Management and Application Hosting*, 18 March 2014

MPTO 00-33A-1114, *AFIN Problem Management*, 26 February 2014

MPTO 00-33A-1202, AFIN *Account Management*, 18 March 2014

MPTO 00-33A-1301-WA-1, *Foreign National NIPRNET Access Core Service*, 4 April 2016

MPTO 00-33B-5004, *Access Control for Information Systems*, 23 July 2015

MPTO 00-33D-2001, *AFNET Naming Conventions*, 17 April 2015

Information Technology Infrastructure Library (ITIL)

Prescribed Forms

USAFA Form 136, *Software Request Questionnaire*

USAFA Form 142, *USAFA Commercial ISP Agreement*

USAFA Form 75, *USAFA Privileged User Agreement*

Adopted Forms

DD Form 2842, *DOD PKI Certificate of Acceptance and Acknowledgement of Responsibilities*

DD Form 2875, *System Authorization Access Request*

AF Form 847, *Recommendation for Change of Publication*

AF Form 4394, *Air Force User Agreement Statement – Notice and Consent Provision*

Attachment 2

USAFA IT SERVICE CATALOG

A2.1. The USAFA IT Service Catalog will be available to USAFA personnel on SharePoint. The service catalog contains approved levels of service for all IT. Any exceptions to levels listed in the service catalog must be submitted through the Service Request Process.

A2.2. The following items shall be developed and maintained as part of the USAFA IT Service Catalog:

A2.2.1. AFNET and USAFA unique operational C&I services currently available to USAFA IT users.

A2.2.2. List of preapproved standard services/changes identified through the IT Change Management Process.

A2.2.3. List of exceptions to policy, waivers, and items identified through the IT Change Management Process.

A2.2.4. Approved applications

A2.2.5. Approved standard changes

A2.2.6. List of approved SLAs

A2.2.7. Approved service changes

A2.2.8. Shared drive allocation limits

A2.2.9. Approved shared drive allocation limitation exceptions

A2.2.10. Shared drive data types

A2.2.11. Approved shared drive data type exceptions

A2.2.12. Mailbox limitations

A2.2.13. Approved mailbox limitation exceptions

A2.2.14. Blocked internet sites/categories

A2.2.15. Approved blocked internet site/category exceptions

A2.2.16. Approved Port Security exceptions

A2.2.17. Approved DOD PPSM Registry Database exceptions

A2.2.18. Link to the Approved Software List

A2.2.19. Link to the CMS

A2.2.20. List of retired services

A2.3. Each item will contain at a minimum the service name, service description, and any instructions specific to acquiring the service or asset.

Attachment 3

USAFA SERVICE DESIGN PACKAGE TEMPLATE

A3.1. Below is a SAMPLE/TEMPLATE for a Service Design Package for Significant Change projects. This is an example of the information needed to begin validation, testing, release and deployment of a significant RFC. This information is not inclusive of all information required. Program Managers should include all requirement information available in order to facilitate a successful RFC.

Figure A3.1. USAFA SERVICE DESIGN PACKAGE TEMPLATE.

PROJECT DESCRIPTION OR TITLE

Project: NUMBER with TITLE

Location: USAFA, CO

SECTION 1
PROGRAM INFORMATION

1. PROJECT DESIGNATOR

(Project Number /CIPS ID Number)

2. PURPOSE

This needs to be a short narrative that explains the purpose of this project. If this is a downward directed project please state so clearly. Also if the project has an aggressive installation schedule include that in here as well. The importance of the installation schedule should be clearly identified.

3. SUMMARY

Summary of efforts required to complete this project. This should give more comprehensive detail of the level of effort required to get this project done and a general explanation of taskings required.

4. COORDINATION / CONTACT INFORMATION

Information for this SDP was obtained during an Engineering Site Survey conducted on DATE, by POC / PHONE of ORGANIZATION. The following personnel were contacted (add lines as needed for additional coordination):

Rank/Name	Org/Osym	Role	Phone
		Technical Engineer	
		Maintenance Activity	
		Project Manager	

SECTION 2

SITING AND PROJECT INSTALLATION DATA

1. SITING DATA

A. Specific Site and Base Locations: Installation work covered by this SDP will occur in Bldgs: ######.

B. The following list identifies specific equipment, cabinet space, ducts and conduits, and circuits/trunks that will be affected by this project:

C. Other:

2. PROPOSED EQUIPMENT INSTALLATION

A. The following equipment will be installed as detailed in the below tables.

Table 2A. Equipment Installations

Equipment	Location (Bldg)	Room	Equipment / Rack#	Qty

B. The following cabling will be installed as detailed in the below tables.

Table 2B. Cabling Installations

Cable Type		Location (Bldg)	Room / Rack (Eqpt #)	Qty
	From			
	To			
	From			
	To			

3. RELATED FACTORS

A. Electromagnetic Interference/Electromagnetic Capability (EMI/EMC) Statement:

B. IF EMCS study will be conducted please provide details.

C. If other testing may be required, please provide details.

SECTION 3

COMMUNICATION-COMPUTER SYSTEM SUPPORT REQUIREMENTS

1. CIRCUIT REQUIREMENTS

2. TELECOMMUNICATIONS SERVICE REQUESTS:

3. LEASED EQUIPMENT REQUIREMENTS:

4. CRYPTO EQUIPMENT:

5. EMSEC SUPPORT REQUIREMENTS:
Coordinate with the USAFA/A6 Cyber Security personnel to ensure EMSEC requirements are identified

6. CABLE WORK
Outside plant cable work will be performed by xxxxxxxxx. Inside plant cabling will be performed by xxxxxxxxxxx

7. IT ARCHITECTURE/TOPOLOGY REQUIREMENT:

8. DOWNTIME:

9. OTHER CONSIDERATIONS
A. Will a technical point of contact from 10 CS/???? will be required during system installation and testing.

B. Installation activity (or more specifically who?) will dispose of project installation residuals.

SECTION 4

CIVIL ENGINEERING SUPPORT REQUIREMENTS

1. SITE WORK AND EXTERIOR UTILITIES

2. BUILDINGS

A. Civil-Architectural Requirements: Host Civil Engineering will be required to provide:

B. Bldgs ####, #### Mechanical Requirements.

1) Design Criteria for Environmental Control, Heat Emission and Ventilation Requirements: Identify the building mechanical requirements by building and room number for equipment installed under this project.

Table 4B. Building Mechanical Requirements

Bldg	Room	Min Operating Temp	Max Operating Temp	Max Humidity	Heat (BTU/hr)	Ventilation (Adequate/ Not Adequate)

2) Special Considerations: SHPO/Environmental?

C. Electrical Requirements.

1) Technical Power: List the power requirements for the equipment to be installed in each building and room.

Table 4C1. Bldg ####Power Requirements

Item	FPI	Voltage	Freq.	Phase	# of Wires	# of Units	Watts

Table 4C1. Bldg ### Power Requirements

Item	FPI	Voltage	Freq.	Phase	# of Wires	# of Units	Watts
NAME	Room ,	110 + 15 VAC	50-60 Hz	Single	1	2	120

Table 4C1. Bldg ### Power Requirements

Item	FPI	Voltage	Freq.	Phase	# of Wires	# of Units	Watts
NAME	Room ,	110 + 15 VAC	50-60 Hz	Single	1	2	120

2) Duct and Conduit: Existing ducting is adequate / REQUIRED?

3) Electrical Wiring: ##-Amp twist-lock electrical connectors will be provided for equipment rack power. ## twist-lock connector for Rooms ## and ## are required; two twist-lock connectors are required for Room ###.

4) Technical Power: Existing technical power will be used/not used?

5) Non-Technical Power Panels:

6) Lighting and Receptacle Requirements:

7) Grounding Requirements: All equipment installed under this project will meet local facility grounding standards.

8) Lighting Protection Requirements:

9) Obstruction Lighting Requirements:

3. RESTORATION OF WORK LOCATION:

4. SURVEY AND STAKE BURIED UTILITIES:

5. COMPLETION DATE:
The anticipated construction completion date is DATE.

SECTION 5

BASE SUPPORT REQUIREMENTS

1. Vehicle Support:

2. Phone Support:
Commercial / Administrative phones.

3. Confined Space Requirements:

4. Restrictions:
Please state any restrictions that this installation may have. This is normally a Not Applicable statement. This should include any escorts that may be required in secure areas.

5. Waivers:
This may be required if the installation is going to require an action that contradicts what the local installation guidance determines. This is normally a Not Applicable statement.

SECTION 6

SCHEDULING REQUIREMENTS

1. Anticipated Allied Support Completion Date:

The anticipated required Allied Support Completion (ASC) date for all support covered in this SDP is TBD. If the ASC date cannot be met, advise POC with Telephone/DSN. The ASC date is for planning purposes only. Do not delay your response to the SDP because of this date. Provide proposed completion or projected completion date as part of your concurrence or non-concurrence so that we may continue our internal processing of this requirement. The project completion date may have to be adjusted if the ASC date is significantly delayed.

2. Anticipated Installation Start Date:
The anticipated Start Date for project installation is DATE. The project is expected to take ### week to complete the installation.

3. Access Locations / Requests
The installation team will require access to USAFA, Bldgs # during what times. This would be good spot for a work breakdown schedule. Who is doing what when?

SECTION 7

FUNDING PROFILE

1. Funding Activity

……TBD……...will provide funding for this project. Project funding will include the cost of the equipment listed in Table (TBD) and the cost of installing this equipment. **P**rovide a description of the proposed cost estimates for planning purposes. Project implementation will include final cost determination and contract award fee allowance

ITEM	APPROP/PURPOSE	FY16	FY17	FY18	FY19
1	3080/Purchase	-0-	-0-	-0-	-0-
2	3080/Purchase	-0-	-0-	-0-	-0-
	3080/Sub Total	$0	$0	$0	$0
3	3400/Purchase		-0-	-0-	-0-
4	3400/Lease	-0-	-0-	-0-	-0-
5	3400/Logistics Support		-0-	-0-	-0-
6	3400/Software Maintenance	-0-	-0-	-0-	-0-
7	3400/Hardware Maintenance	-0-	-0-	-0-	-0-
8	3400/Site Prep		-0-	-0-	-0-
9	3400/Training, TDY & Others		-0-	-0-	-0-
10	3400/Site Support	-0-	-0-	-0-	-0-
11	3400/Minor Hardware (est)	-0-	-0-	-0-	-0-
12	3400/C4 Support		-0-	-0-	-0-
	3400/Sub Total	$	$0	$0	$0
	Total		$0	$0	$0

2. Training Costs:

Include a statement or section that will explain if training will be required. If so indicate who requires it and what the cost will be. Include who will be responsible to fund for any additional training that might be required. .

SECTION 8

MAINTENANCE / SUSTAINMENT

1. Maintenance Strategy

……TBD……...will provide funding for this project. Project funding will include the cost of the equipment listed in Table (TBD) and the cost of installing this equipment.

SECTION 9

SECURITY AND ACCREDIDATION

1. ……TBD……...will develop a network Authority to Operate Accreditation Package.

2. ……TBD……...will maintain the network Authority to Operate Accreditation Package.

3. If accreditation is required, specify who will be the responsible agency. At a minimum the local Cybersecurity Liaison should review all A&A documents and ensure all procedures are being followed.

4. System Information System Owner for new system: _____

5. System Program Manager for new system: _____

6. Functional System Administrator for new system: _____

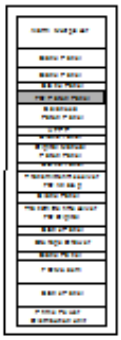
SECTION 10

DRAWINGS

FIGURE	DRAWING TITLE	LOCATION
Figure 1		
Figure 2		
Figure 3		

Rack #
Figure Number xx.xx

Be fore



After

LIST

Item	Source (POC/Contract Vehicle)	Manufacturer	Part #	Description	Qty	Unit Price	Total Price
				Total			$

Authored and Submitted By:

_____ _____
<<Program Manager's Name Here>> Date
<<PMs Title Here>>
Org/Off Sym

Reviewed By:

_____ _____
<<Lead, C4 Engineering Name Here>> Date
<<Lead's Title Here>>

Reviewed By:

_____ _____
<<Customer Commander/Director Name Here>> Date
<<Title Here>>
<<Organization Here>>

Allied Support Concurred By:

_____ _____
10th Civil Engineering Squadron Date